Data Retention Policy

1. Purpose, Scope and Users

This policy sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within Headland Archaeology (further: the "Company").

This Policy applies to all offices, processes, and systems, where the Company conducts business and has dealings or other business relationships with third parties.

This Policy applies to all Company officers, directors, employees, agents, partners, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and/or sensitive personal data). It is the responsibility of all of the above to familiarise themselves with this Policy and ensure adequate compliance with it.

This policy applies to all information used at the Company. Examples of documents include:

- Emails
- Hard copy documents
- Soft copy documents
- Video and audio
- Data generated by physical access control systems

2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Personal Data Protection Policy

3. Retention Rules

3.1. Retention General Principle

In the event of any category of documents not specifically defined elsewhere in this Policy (and in particular within the Data Retention Schedule) and unless mandated differently by applicable law, the required retention period for such document will be deemed to be 3 years from the date of creation of the document.

3.2. Retention General Schedule

The Data Protection Officer defines the time period for which the documents and electronic records should to be retained through the Data Retention Schedule.

As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from authorities, if there is a chance records of personal data are needed by the Company to prove compliance with any legal requirements; or
- When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law.

3.3. Safeguarding of Data during Retention Period

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during

the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes.

The responsibility for the storage falls to the Data Protection Officer and the compliance team.

3.4. Destruction of Data

The Company and its employees should therefore, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See Appendix for the retention schedule. Overall responsibility for the destruction of data falls to the Data Protection Officer.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data Protection Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the Company's Personal Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevents the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the company's IT Security Policy.

The Data Protection Officer shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

3.5. Breach, Enforcement and Compliance

The person appointed with responsibility for Data Protection, the Data Protection Officer has the responsibility to ensure that each of the Company's offices complies with this Policy. It is also the responsibility of the Data Protection Officer to assist any local office with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to Data Protection Officer. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate. Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to the Company's reputation, personal injury, harm or loss.

Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Company premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

4. Document Disposal

4.1. Routine Disposal Schedule

Records which may be routinely destroyed every quarter, unless subject to an on-going legal or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies;
- Requests for ordinary information such as travel directions;
- Reservations for internal meetings without charges / external costs;
- Transmission documents such as letters, fax cover sheets, e-mail messages, routing slips, compliments slips and similar items that accompany documents but do not add any value;
- Superseded address list, distribution lists etc.;
- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files;
- Stock in-house publications which are obsolete or superseded; and
- Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organizations.

In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.

4.2. Destruction Method

Level I documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

Level II documents are proprietary documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be cross-cut shredded and then placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

Level III documents are those that do not contain any confidential information or personal data and are published Company documents. These should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

5. Managing Records Kept on the Basis of this Document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data Retention Schedule	Data Protection Officer's Server Folder	Data Protection Officer	Only authorised persons may access this document	Permanently

6. Validity and document management

This document is valid as of May 2018

The owner of this document is the Data Protection Officer who must check and, if necessary, update the document at least once a year.

7. Administration

Below as Appendix is a Record Retention Schedule that is approved as the initial maintenance, retention and disposal schedule for physical records of The Company and the retention and disposal of electronic documents.

We will make modifications to the Record Retention Schedule from time to time to ensure that it follows the legislation and includes the appropriate document and record categories for The Company; monitor legislation affecting record retention; annually review the record retention and disposal program; and monitor compliance with this Policy.

In addition, any retained information can only be used for the purpose for which it is stored. This is compliant with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

8. Appendices

Appendix – Data Retention Schedule

The Record Retention Schedule is organised as follows:

SECTION TOPIC

1. **Accounting and Finance**
2. **Contracts**
3. **Corporate Records**
4. **Correspondence and Internal Memoranda**
5. **Personal Information & Personnel Records**
6. **Electronic Records**

1. Accounting & Finance Records | Owner: Finance

Record type	Retention period
Pay & tax: HMRC correspondence, PAYE records, maternity and paternity pay records	3 years after the end of the financial year to which they relate
Tax returns	10 years from end of fiscal year
Accounting & financial management information, personal data, complaints, employment records, legacies, intellectual property, pay & tax, pension information, risk & insurance	6 years from end of fiscal year
Supplier contracts	7 years after contract is terminated
Fiscal Policies and Procedures	Permanent

Annual audit reports and financial statements	Permanent
Annual audit records, including work papers and other documents that relate to the audit	7 years after completion of audit
General Ledger	Permanent
Investment records (deposits, earnings, withdrawals)	7 years
Asset registers, receipts, purchase orders, invoices - revenue, petty cash, creditor's & debtor's records; benefits in kind; draw results; standard T&Cs, software licenses, management accounts, successful grant applications and correspondence	7 years after last action
Credit card receipts	3 years
Tax or employee identification number designation	Permanent
Annual corporate filings	Permanent

2. Contracts | Owner : Contracting Management & Sales

Record type	Retention period
Signed	Permanent
Contract amendments	Permanent
Successful tender documents	Permanent
Unsuccessful tenders' documents	Permanent
Tender – user requirements, specification, evaluation criteria, invitation	Permanent
Contractors' reports	Permanent
Operation and monitoring, eg complaints	Permanent

Client's data, information relating to any subscriptions made, or serving business purposes (PR methods, business cards etc)	Indefinitely whilst organisation remains a client. Once an organisation requests all records to be deleted, data will be removed from the back-ups within 9 months

3. Corporate Records | Owner: Company Secretary

Record type	Retention period
Article of Incorporation to apply for corporate status	Permanent
Board policies	Permanent
Board meeting minutes	Permanent
Annual reports & accounts, press releases and cuttings, register of members, memorandum of association, register of directors and secretaries, employer's liability insurance certificates, licenses & permits	Permanent
Court orders	Permanent
Legal files	1 year after expiration of appeals or time for filing appeals
Material of historical value (including pictures, publications)	Permanent
Policy and Procedures manual	Current version with revision history

4. Correspondence & internal memoranda | Owner: Administration and staff

General Principle: Most correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support. For instance, a letter or email pertaining to a particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded within five years. Some examples include:

    - Routine letters and notes that require no acknowledgment or follow up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings

- Form letters that require no follow up
- Letters of general inquiry and replies that complete a cycle of correspondence
- Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change)
- Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary
- Chronological correspondence files
- Please note that copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed, unless that information provides reference to or direction to other documents and must be kept for project traceability

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.

5. Retaining Personal information & Personnel Records | Owner : HR

This Section sets out the data retention policies and procedure of The Company, which are designed to help ensure compliance with legal obligations in relation to the retention and deletion of personal information

Personal information that is processed by The Company for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Without prejudice to point 2 (above) The Company will usually delete personal data falling within the categories set out below at the date/time set out below:

Record type	Retention period
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals	6 years after employment ceases
Applications for jobs, interview notes – Recruitment/promotion panel Internal Where the candidate is unsuccessful Where the candidate is successful	1 year after last action Duration of employment
Consent forms, image consent forms, parental consent, release forms, subject access requests, notifiable disease, insurance claims	3 years from last action
Employment records: redundancy, equal opps; health & welfare records; pay & tax: pay deductions, tax forms, payroll, loans, payroll input forms, wages/salary records, overtime/bonus payments Payroll sheets, copies	6 years
Personnel files and training records	6 years after employment ceases
Statutory Sick pay records, calculations, certificates, self-certificates	The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) abolished the former

	obligation on employers to keep these records. Although there is no longer a specific statutory retention period, we still have to keep sickness records to best suit our business needs, therefore records will be kept for 6 years after the employment ceases.
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
Bank details – current	Duration of employment
Payrolls/wages	Duration of employment
Job history including staff personal records: contract(s), Ts & Cs; previous service dates; pay and pension history, pension estimates, resignation/termination letters	6 years from the end year
Employee address details	Duration of employment
Annual leave records	Duration of employment
Accident books Accident reports and correspondence	3 years from the date of the last entry (or, if the accident involves a child/young adult, then until that person reaches the age of 21) – H&S
Assessments under H&S regulations and records of consultations with safety representatives and committees	Permanently – H&S
Parental leave	18 years from the birth of the child
Maternity pay records and calculations	3 years after the end of the tax year in which the maternity period ends
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy
Training and development records	Duration of employment
Medical & health records	30 years after employment ceases

Medical records under the control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos and medical examination certificates	40 years from the date of the last entry; (medical examination certificates) 4 years from the date of issue
Annual return, job descriptions,	3 years from last action

6. Electronic Documents | Owner: Individual employee

Record type	Retention period
Recycle Bins	Cleared monthly
Downloads	Cleared monthly
Inbox	All emails containing PII attachments deleted after 3 years.
Deleted Emails	Cleared monthly
Personal Network Drive	Reviewed quarterly, any documents containing PII deleted after 3 years
Local Drives & files	Moved to network drive monthly, then deleted from local drive
Google Drives, One Drive, Drop box	Reviewed quarterly, any documents containing PII deleted after 3 years

The Company does not automatically delete electronic files beyond the dates specified in this Policy. It is the responsibility of all staff to adhere to the guidelines specified in this policy.

In certain case's a document will be maintained in both paper and electronic form. In such cases the official document will be the electronic document.