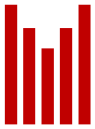

MILLENNIUM

HOTELS AND RESORTS

MILLENNIUM ▪ COPTHORNE

Global
Data Retention & Disposal Policies

Table of Contents

RECORD RETENTION POLICY

1. PURPOSE

1.1 This Policy defines the minimum requirements for the maintenance, storage, retrieval and retention of Records held by Millennium & Copthorne Hotels Plc and its direct and indirect subsidiaries ("MHR").

1.2 MHR is committed to managing Records in a manner which complies with applicable laws and meets the information retention and retrieval needs of its operations. This Policy, together with the record retention schedule set out at Annex A (the "Record Retention Schedule"), describes MHR's Record management procedures.

1.3 MHR expects all employees to fully understand and comply with this Policy and the Retention Schedule. This Policy and the Retention Schedule also applies to all MHR's contractors, vendors, and any other person using or accessing MHR's information or information systems. No policy, however, can cover every Record management issue or situation that may arise. Any questions regarding Record management and retention issues not covered by this Policy should be addressed to the MHR Legal Team.

1.4 MHR will make all reasonable endeavours to keep Records accurate, reliable, ordered, complete, useful, up to date, accessible and will only retain Records where necessary to achieve one or more purposes, including the following:

(a) helping us carry out or achieve our strategy and deliver high quality support and services;

(b) helping us to make informed decisions;

(c) protecting the rights of employees and the public;

(d) tracking policy changes and development;

(e) making sure we comply with relevant legislation;

(f) providing an audit trail to meet business, regulatory and legal requirements;

(g) supporting business continuity and consistency in management and administration;

(h) making sure we are open, transparent and responsive;

(i) supporting research and development; and

(j) promoting our achievements.

2. DEFINITIONS

The following definitions apply to this Policy:

"**Record Retention Schedule**" means the Record Retention Schedule set out at Annex A to this Policy;

"**GDPR**" means the EU General Data Protection Regulation (GDPR) (EU) 2016/679;

"**Personal Data**" means data relating to a living individual who can be identified from the data or from other information currently or likely to come into, the possession of MHR. Personal Data can be factual or opinion-based; and

"**Records**" means all and any records or documents, in any format, containing business data relating to MHR or Personal Data collected or processed by MHR, and includes paper documents, including but not limited to final versions, drafts, correspondence, handwritten notes, and diary entries, as well as video and audiotapes and all computer files, e-mail, and other documents or data in electronic form on hard drives, servers, disks, back-up tapes, hand-held devices, or any other media or devices.

3. RELATED POLICIES

This policy should be read along with all other relevant MHR policies, including; without limitation the following information security/data protection policies:

- Privacy Notice (EU) for Employees, Workers and Contractors
- Global Data Protection Policy
- Data Protection Guidance
- Data Subject Access Rights Policy
- Global Information Security Policy
- Data Breach Reporting and Management Policy

4. PROCEDURE

4.1 MHR requires certain types of Records to be retained for specified periods in compliance with applicable laws. These Records must be managed in accordance with the procedures outlined in this Policy and the Record Retention Schedule. In all circumstances however, the following exception overrides the time periods in the Record Retention Schedule: If you have reason to believe that MHR Records are relevant to an actual or potential lawsuit or government investigation, you must preserve those Records until you are notified otherwise by the Legal department.

4.2 MHR's policy is to maintain Records for the periods stated in the Record Retention Schedule unless a legal exception applies, referred to in Section 4.1 of this Policy.

4.3 Personal Data shall be retained and processed in accordance with Section 5 of this Policy.

4.4 MHR may choose to comply with legal requirements by storing certain Records electronically. This will not, however, change the required retention period.

5. ROLES & RESPONSIBILITIES

MHR has a responsibility to ensure that all Records are managed appropriately and in accordance with this Policy. Personnel have different roles in relation to the management of Records, depending on their role within MHR. These responsibilities are detailed below:

5.1 The designated Regional Compliance Teams –will have responsibility for ensuring compliance with this Policy. Individual members have responsibility for ensuring that their assigned/respective departments have procedures in place to comply with the Policy and shall be responsible for ensuring the Record Retention Schedule is kept up to date by the various departments.

5.2 Department Heads shall be responsible for:

(a) identifying specific Records listed in the Record retention schedule;

(b) identifying Records which are required to meet business regulations;

(c) establishing methods for orderly processing, filing, identifying, labelling, storing and maintaining Records;

(d) implementing appropriate security measures to prevent unauthorised changes, removal or access to Records;

(e) disposing of Records in accordance with the Record Disposal Policy when the applicable Record retention period expires; and

(f) recommending changes to the Record Retention Schedule where they identify a need to retain Records for longer than the prescribed retention period, or they identify that the prescribed retention periods are unjustifiably long.

5.3 Global Director of Risk Management & Compliance is responsible for:

(a) considering and approving changes to this Policy;

(b) ensuring that this Policy and the Record Retention Schedule are reviewed on an annual basis and remains relevant;

(c) raising staff awareness of Record management;

(d) providing advice and guidance relating to this Policy to line managers and staff; and

5.4 **All staff, volunteers and contractors** are responsible for ensuring that Records they receive, create, maintain or delete are dealt with in accordance with this Policy and the Record Retention Schedule.

6. RECORDS CONTAINING PERSONAL DATA

6.1 Personal Data shall be processed in accordance with the following data protection principles:

Personal Data shall be:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date - every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed; and

(f) processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6.2 Records containing Personal Data must be:

(a) stored appropriately having regard to the sensitivity and confidentiality of the material recorded;

(b) retrievable and easily traced;

(c) retained for only as long as necessary and in accordance with Section **Error! Reference source not found.** of this Policy;

(d) disposed of appropriately and to prevent Records falling into the hands of unauthorised personnel;

(e) considered as confidential in nature.

7. STORAGE AND TRANSPORT OF DATA

7.1 All Records should be stored and, where applicable, transported as securely as possible in order to avoid potential misuse or loss. All Records will be stored in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the Record.

7.2 The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded. Any HR Records, or Records which are marked 'confidential', 'sensitive', 'internal use only' or similar, will be kept in a secure cabinet accessed only by authorised personnel.

7.3 Records which are active should be stored in the most appropriate place for their purpose.

7.4 Records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose.

8. RETENTION PERIOD

8.1 Record retention is necessary for compliance and in order to protect MHR's interests.

8.2 The period for which Records should be retained varies according to the nature of the Record. Relevant periods are set out in the Record Retention Schedule. The period of retention commences when the Record has been used for its original purpose and has been stored whether electronically or in paper form.

8.3 Retention periods will vary and will be dependent on:

(a) the type of Record;

(b) the original purpose for which the Record is created or received;

(c) whether MHR is still using the Record in accordance with the original purpose; and

(d) whether MHR has reason to retain the Record for a different purpose in the future.

8.4 The following general principles should be considered when determining retention periods:

(a) Is the Record significant in terms of development or policy change or HR (e.g. minutes of meetings, contracts, employee Records)?

(b) Does the Record relate to a transaction which set, or is likely to set, a precedent?

Example: Versions of contracts

(c) Does the Record contain data which would be useful for retrospective comparisons?

Example: Company P&L and associated Records.

(d) Does the Record contain systematically recorded data which is not easily available elsewhere?

Example: Management Agreements Records and statistics.

(e) Does the Record contain information gathered from outside MHR?

Example: statistics from competitors

(f) Is the Record likely to be useful as legal evidence in the future?

Example: papers relating to disputes or HR Issues

8.5 Retention periods in relation to Personal Data shall be set at an initial maximum period, following which a review will take place to consider whether the Record should be retained for a further period, as follows:

(a) The GDPR does not specify a maximum period of time MHR can retain Personal Data; however, in order to meet its obligations under the GDPR, MHR considers three years to be the maximum period of time Records containing Personal Data can be retained before there must be a review of the Record. A shorter period or a longer period may be appropriate depending on the kind of Personal Data being stored. The Head of the relevant department is responsible for conducting a review each January and to determine whether a Record containing Personal Data should be deleted.

(b) Any review must involve identifying the original purpose for which the Personal Data was collected, determining whether the Record should be deleted or retained and if so, for what reason.

(c) Where a Record containing Personal Data is identified that exceeds the retention periods listed below, that Record must be disposed of in accordance with the Record Disposal Policy unless there is a justified reason for further storage.

8.6 Following the review referred to in Section 8.5, Records containing Personal Data shall be retained for a further maximum period, as follows:

(a) Six years should be regarded as the maximum period of time Records containing Personal Data can be retained. Excluding Records relating to workers, no Records containing Personal Data should be retained for longer than six years, unless it can be demonstrated that there is justified reason for doing so. Reasons for longer retention can include:

- where there is a threat of litigation. Records should not be destroyed, deleted or disposed of until the threat has been removed;
- the Records contain information relevant to legal action which has already started or in contemplation. Such Records should be retained until any legal action has come to an end or it has been decided that no further legal action is going to occur;
- where a business relationship comes to an end, Records in respect of that relationship may need to be retained to defend any legal claims; or
- where statutory exemptions apply or the law requires retention for a longer period.

8.7 MHR will review whether it has a reason to keep Records containing Personal Data for longer than the maximum retention period described in Section 8.6 annually and ahead of the expiration of the any minimum retention period set out in the Record Retention Schedule. However, if you become aware of any Personal Data that is being held beyond the maximum retention period described in Section 8.6, please contact the Global Director of Risk Management and Compliance. Where appropriate and in line with any changes in its business functions, MHR will also review the maximum periods of retention as set-out in this Policy.

9. LEGAL EXCEPTION -MODIFICATION OF DOCUMENT RETENTION PERIODS

9.1 In the event that:

(a) MHR receives notice that it or a director, officer, or employee has been made a party to litigation or an investigation by a governmental department or agency,

(b) MHR reasonably anticipates that it, or a director, officer, or employee, may be party to litigation or that there is potential for a governmental investigation or proceeding related to company activities, or

(c) MHR or an affiliate, or a director, officer, or employee, receives a court order requesting documents,

MHR will implement a plan to preserve relevant records.

9.2 MHR's Legal Department should be consulted in connection with any decision on whether documents should be preserved in response to a legal matter. In the event that normal document retention procedures may need to be suspended for legal reasons, a "Litigation Hold Notice" or other written notice from the Legal Department will be sent to MHR or an affiliate, or a director, officer, or employee.

9.3 If any employee learns of information suggesting that there is any actual or potential litigation, investigation, or other proceeding against or involving MHR or a director, officer, or employee, the employee must immediately notify the Legal Department

9.4 No director, officer or employee of MHR shall destroy any document relevant to the subject matter of the investigation or litigation without specific written authorisation from the Legal Department.

9.5 Known destruction by any MHR employee of documents related to a pending or anticipated civil or criminal proceeding or investigation may be grounds for disciplinary action up to and including possible termination of employment. Further, such conduct may subject the employee to civil and criminal penalties.

9.6 The Legal Department shall inform all personnel who have been instructed for legal reasons to suspend MHR's usual document destruction procedures when it is appropriate to resume those usual procedures.

9.7 Any questions regarding retention of documents, including whether a legal matter requires suspension of MHR's usual document destruction procedures or whether specific documents are relevant to a legal matter, should be directed to the Legal Department.

10. DESTRUCTION, DELETION & DISPOSAL

Any Records which are not required to be retained in accordance with this Policy must be securely destroyed in accordance with the Record Disposal Policy.

11. CHANGES TO THE RETENTION POLICY

Upon review, MHR will update this Policy to reflect any changes to its internal procedures and requirements, including any changes in to the maximum retention periods.

RECORD DISPOSAL POLICY

1. PURPOSE

1.1 The destruction, deletion and disposal (collectively referred to in this policy as "**disposal**") of Records by MHR must take place safely and securely in order to comply with various statutory and other requirements including, in respect of Records containing Personal Data, the GDPR. It is very important to ensure that, for both statutory and reputational reasons, Records do not fall into the hands of unauthorised personnel or third parties.

1.2 Definitions used in the Record Retention Policy are used in this Policy.

2. RELATED POLICIES

This policy should be read along with all other relevant MHR policies, including; without limitation the following information security/data protection policies:

- Privacy Notice (EU) for Employees, Workers and Contractors
- Global Data Protection Policy
- Global Data Protection Guidance
- Global Data Subject Rights Policy
- Global Information Security Policy
- Global Data Breach Reporting and Management Policy

All data protection policies, including all the above, can be found at https://www.millenniumhotels.com/en/corporate/grouppolicies/.

3. SCOPE

3.1 This Policy outlines MHR's policy on the disposal of Records, which should take place following the expiry of the retention periods applicable to the relevant Records. The Record Retention Policy, together with the Record Retention Schedule, sets out when and for how long Records should be kept.

3.2 This Policy specifies acceptable disposal methods for Records held in any format and on any media, including but not limited to:

(a) Hard disk;

(b) CD and DVD;

(c) Solid state devices such as USB's and memory cards;

(d) Network drives, servers or 'cloud' storage

(e) Paper, including faxes, post-it notes, etc.

3.3 Unless there is a business case or legal obligation for continued retention, all Records must be disposed of in a secure and appropriate manner following the expiry of the retention periods specified in the Record Retention Policy and/or the Record Retention Schedule.

4. DISPOSAL OF PAPER RECORDS

4.1 All paper Records should be disposed of in a secure but environmentally-friendly manner using boxes or bins provided in MHR's offices. Records that contain Personal Data or are confidential sensitive in nature should be disposed of in bins marked 'confidential waste' or similar. MHR will ensure that the contents of bins marked 'confidential waste' will be shredded in such a way that it cannot be put back together again. Such shredding will take place at least once per month by a document disposal company which will undertake such shredding according to confidential handling requirements in their disposal agreements.

4.2 MHR maintains an electronic register of key or significant paper Records (for example, an original contract) which have been identified for disposal. This register is maintained by the Legal Department. Prior to the disposal of such Records, you should update the register by contacting the Legal Department. You should not dispose of such Records until the Legal Department has authorised you to do so.

5. DISPOSAL OF ELECTRONIC RECORDS

5.1 Electronic Records should be disposed of by the deletion of files/data at an application or operating system level. This should be performed such that the deleted files/data cannot be retrieved by simply undoing the last action or restoring the item in the recycle bin. Back-ups of all such electronic Records should be dealt with in the same manner.

5.2 Subject to Section 5.4, where any electronic device or media (including but not limited to PCs, laptops, mobile phones or USB sticks) are to be recommissioned, MHR's IT Department should run a low-level format of the device prior to re-commissioning the unit within MHR.

5.3 Where any electronic device or media (including but not limited to PCs, laptops, mobile phones or USB sticks) are due to be decommissioned, the electronic device shall be disposed of (and in no circumstances offered for resale) by the use of a certified data destruction company, which shall involve the following process:

(a) secure pickup of the device;

(b) destruction of the device through de-gaussing, incineration or shredding;

(c) certification of device destruction; and

(d) recycling/disposal of remaining components in accordance with environmental regulations.

5.4 Special considerations apply to the disposal of confidential or sensitive Records (including those containing Personal Data) stored on electronic devices or media (including but not limited to PCs, laptops, mobile phones or USB sticks). Accordingly, such Records shall be disposed of by the IT department performing a "secure wipe" of the device or media using appropriate software. This process shall also be followed where electronic devices or media are being 'overwritten' by saving new Records to the device or media; the process of saving new Records may overwrite areas of the device or media, but this is no guarantee of preventing retrieval of previously stored Records.

5.5 MHR maintains an electronic register of key or significant electronic Records (for example, copies of contracts) which have been identified for disposal. This register is maintained by the Legal Department. Prior to the disposal of such Records, you should update the register by contacting the Legal Department. You should not dispose of such Records until the Legal Department has authorised you to do so.

6. LARGE VOLUME DISPOSAL

6.1 If there is a substantial quantity of Records due for disposal (i.e. a repository of Records which are stored past the relevant retention periods has been identified) a one-off destruction is potentially appropriate. In this case, the following procedures apply:

(a) clearly document what Records are being considered for possible disposal;

(b) review a representative sample to determine content and the appropriateness of disposal;

(c) classify the Records into groups where possible;

(d) verify with the Legal Department that none of the Records should be retained for purposes of any current or anticipated litigation or investigation. If the Legal Department identifies Records as having to be retained for any such legal purpose, those Records shall be retained in strict accordance with the Legal Department's instructions;

(e) prepare a description of each group of Records to be disposed of and circulate the description to appropriate department managers to get approval;

(f) once all necessary approvals are obtained, follow the procedures for disposal described in Sections **Error! Reference source not found.** and 5, including updating the register of disposed Records in accordance with the procedure set out in Sections 4.2 and 5.5; and

(g) document the disposal including date, description of groups destroyed, method of destruction, and individuals involved and provide such documentation to the Legal Department.

APPENDIX A

RECORD RETENTION SCHEDULE

This Record Retention Schedule includes a non-exhaustive list of the main categories of Records held by MHR (in whatever format or media). If you have queries about specific Records please contact the Legal department.

As a general rule, all Records that do not need to be retained should be disposed of in accordance with MHR's Data Disposal Policy as soon as possible after its receipt, creation or use in accordance with the specified purpose for which it was collected.

However, many types of Records will need to be kept for a minimum period to satisfy various statutory and regulatory requirements or for other business reasons. In accordance with MHR's Record Retention Policy, Records containing Personal Data shall be kept for no longer than the maximum retention periods set out below unless there is an appropriate reason for doing so.

It is the responsibility of the Head of the department to ensure that Records containing Personal Data are either retained or deleted in accordance with MHR's Record Retention and Disposal Policies.

Appendix A: MHR Data Retention Schedule- UK

CATEGORY	RELEVANT LEGAL RULE	DESCRIPTION	START OF THE RETENTION PERIOD	REQUIRED PERIOD OF RETENTION
1.Tax and Accounting Records **Purchase invoices and supplier documentation**	Companies Act	Accounting records	Relevant year end	Six years from year end
	VAT Act HMRC Notice 700/21 (October 2013)	Reports and accounts Records of all delivery of goods or services, all intra-European Community acquisitions, all imports and exports, and all other information relevant for VAT purposes General obligation to keep at least the following records: (i) VAT invoices sent and received; (ii) documentation relating to supplies and acquisitions within the EU; (iii) documentation relating to goods imported from, and exported to, outside the EU. More specifically, the following records should be kept: annual accounts (including profit and loss accounts), bank statements and paying-in slips, cash books and other account books, credit or debit notes you issue or receive, documentation relating to dispatches / acquisitions of goods to/from EC Member States, documents or certificates supporting special VAT treatment such as relief on supplies to visiting forces or zero-rating by certificate, import and export documents, orders and delivery notes, purchase and sales books, purchase invoices and copy sales invoices, records of daily takings such as till rolls, relevant business correspondence and VAT accounts.	Date which records were made	Six years
	The Income Tax Regulations	Income tax and NI returns, income tax records and correspondence with the Inland Revenue	The end of the financial year to which they relate	Not less than 3 years
	Companies Act	Payments cash book or record of payments made	The end of the financial year in which the transaction was made	Six years
	Companies Act	Purchase ledger		
	Companies Act	Invoice - revenue		
	Companies Act and HMRC	Petty cash records		
	Companies Act and HMRC	Invoice – capital item	From invoice receipt	Ten years

	Commercial considerations	Successful quotations for capital expenditure	N/A	Permanently
2. Employment Records **Personnel Records** **Human Resource Documents** **Payroll documentation**	Best practice	Works council minutes	N/A	Permanently
	Limitation Act Data Protection Act	Employment contracts	Date employment ceases	Six years, unless document executed as a deed, in which case 12 years
	Taxes Management Act 1970	Income tax records re employees leaving i.e. P45	Date employment ceases	Six years plus current year
	Taxes Management Act 1970	Notice to employer of tax code (P6)	Date employment ceases	Six years plus current year
	Taxes Management Act 1970	Annual return of employees and directors expenses and benefits (P11D)	Date employment ceases	Six years plus current year NB. According to Lexis the general time limit under the TMA 1970 was due to reduce to four years from 1 April 2012)
	Taxes Management Act 1970	Certificate of pay and tax deducted (P60)	Date employment ceases	Six years plus current year
	Taxes Management Act 1970	Notice of tax code change	Date employment ceases	Six years plus current year
	Taxes Management Act 1970	Annual return of taxable pay and tax deducted	Date employment ceases	Six years plus current year
	Pensions Act	Records of pension deductions (including superannuation)	Date employment ceases	Six years plus current year
	Audit	Clock cards	Following audit	Two years
	Companies Act and Taxes Management Act	Payroll and payroll control account	Date employment ceases	Six years plus current year
Employee/ personnel records	The Control of Lead at Work Regulations	Medical records and details of biological tests under the control of Lead at Work Regulations	Date of last entry	Forty years
	Control of Substances Hazardous to Health Regulations 2002, SI 2002/2677	Register of employees who work with 3rd and 4th category biological agents	Date of last entry in the record	40 years
	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995	Accident reports	Date of last entry or end of investigation if later	Three years If the accident involves a child/young adult, until that child reaches 21 years old
	Commercial	Details of medical schemes	N/A	Permanently
	Commercial	Organisation charts	N/A	Permanently
	Limitation Act	Staff personnel records	Date employment ceases	Six years after employment cease

	Taxes Management Act	Wages and salary records	Date employment ceases	Six years plus the current year
	Taxes Management Act	Expense accounts/records	Date employment ceases	
	Taxes Management Act	Overtime records/authorisation	Date employment ceases	
	Data Protection Act Limitation Act	Redundancy details, calculations of payments, refunds, notifications to the Secretary of State	Date employment ceases	Six years
	Data Protection Act	Life Assurance expression of wish forms	Date employment ceases or death	Six years
	Discrimination Acts 1975 and 1986 and Race Relations Act 1976 recommend six months One year limitation for defamation actions under Limitation Act ICO Employment Practices Code Equality Act 2010	Applications for jobs-where the candidate is unsuccessful	Date notify unsuccessful candidate	Twelve months
	The Statutory Maternity Pay Regulations	Statutory Maternity Pay records, calculations or other medical evidence paternity and shared parental pay records, calculations, certificates or other evidence	End of the tax year in which maternity period ends	Three years
	Statutory Sick Pay (General) Regulations	Sickness records	End of each tax year for Statutory Sick Pay purposes	Three years
	The Retirement Benefits Schemes (Information Powers) Regulations	Records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents	End of scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed.	6 years
	Immigration Restrictions on Employment) Order 2007/3290	Identification documents of foreign nationals (ensuing from the obligation to retain copies of documents used to perform immigration checks)	Date of termination of employment	Two years
Pension records	Commercial	Details re current pensioners	Date benefit ceases	Ten years
	Data Protection Act	Pension scheme – next of kin / expression of wish forms	Date of death	Six years
	Companies Act, Commercial,	Financial records on occupational pension scheme	Date of end of scheme	Six years

	Pensions Act			
	Companies Act, Commercial, Pensions Act	All trust deeds and rules	N/A	Permanently
	Companies Act, Commercial, Pensions Act	Trustees' minute book	N/A	Permanently
	Companies Act, Commercial, Pensions Act	Annual accounts	N/A	Permanently
	Companies Act, Commercial, Pensions Act	Investment & insurance policy records	N/A	Permanently
	Companies Act, Commercial, Pensions Act	Actuarial reports	N/A	Permanently
	Companies Act, Commercial, Pensions Act	Contribution records	N/A	Permanently
3. Board and Board Committee Materials	Companies Act	Register of directors and secretaries	N/A	Life of company
	Companies Act	Certificate of incorporation	N/A	Life of company
	Companies Act	Memorandum of association – signed copies of the original copies	N/A	Life of company
	Companies Act	Articles of association – signed copies of the original copies	N/A	Life of company
	Companies Act	Shareholder agreement	N/A	Life of company
	Companies Act Limitation Act	Directors' service contracts	Date of termination or expiry	Six years Unless executed as a deed, in which case 12 years
	Companies Act	Annual return	From submission date	Three years
	Data Protection Act Companies Act 2006	Trustee/director/governor minutes of meetings and decisions Board Meetings	 Date of meeting	Permanently 10 years
	Data Protection Act	Annual accounts and annual review	N/A	Permanently
	Companies Act, commercial	Investment certificates	N/A	Permanently
	Companies Act, commercial	Investment ledger	N/A	Permanently
	Companies Act, commercial	Fixed assets register	N/A	Permanently

4. Legal Files **Contracts and Agreements**	Limitation Act	Contract with customers, suppliers or agents, licensing agreements, rental/hire purchase agreements, indemnities and guarantees and other agreements or contracts	Date of expiry or termination of contract	Six years If the contract is executed as a deed, the limitation period is twelve years
	Data Protection Act	Major agreements of historical significance	N/A	Permanently
5. Buildings, plant and engineering **Property records**	Data Protection Act	Deeds of title	N/A	Permanently or until property disposed of
	Limitation Act	Leases	Date of expiry	Fifteen years
	Data Protection Act	Final plans, designs and drawings of buildings, planning consents, building certifications, collateral warranties, records of historical interest and final health and safety file.	Date property disposed of	Permanently or until six years after property disposed of
	Limitation Act	Specifications – project document for new buildings and improvements	From date of document creation	Up to twenty-five years
	Limitation Act	Tender documents	Date of project completion	Fifteen years after project completed
	Limitation Act	Agreements with contractors and consultants	Date of project completion	Fifteen years after project completed
	Limitation Act	Surveys and inspections	N/A	Permanently
	Limitation Act	Maintenance contracts and related files	Date of end of contract	Six/twelve years
	Control of Asbestos at work Regulations	Asbestos Register and Asbestos Disposal Certificates	Date of the last entry made in the record	40 years
	Data Protection Act	Hazardous substances: disposal of heavy metals and radioactive sources	N/A	Permanently
	Data Protection Act	Plant and Machinery	Date plant and machinery removed from the building	Until one year
	Data Protection Act	Records of major refurbishments, warranties, planning consents, design documents, final health and safety file	From signature date	Thirteen years for actions against contractors etc
6. Insurance	Data Protection Act	Policies, renewal notices and certificates	Date of lapse	Three years
	Data Protection Act	Claims correspondence	Date of settlement	Three years

	Employers' Liability Regulations	Employer's Liability insurance certificate	Expiry of relevant insurance policy	Forty years or as long as necessary to protect the company's legitimate interests in the event of any potential liability claim or litigation
	Data Protection Act	Accident reports and relevant correspondence	Date of settlement	Three years
	Personal injury actions must generally be commenced within three years of injury. However industrial injuries not capable of detection within that period (e.g. asbestos) the time period may be substantially extended.	Health and safety records	From date of incident	Three years for general records. Permanently for records relating to hazardous substances.
7. Environment	Regulation 1272/2008/EC Regulation 1907/2006/EC (REACH)	Data regarding chemicals or environmentally dangerous substances, and preparations for these which a company has manufactured, imported or supplied	Date the manufacturer, importer, downstream user and distributor last manufactured, imported, supplied or used the substance or preparation	Ten years
	Regulation 1272/2008/EC	The names and addresses of the clients/buyers of the above mentioned substances and preparations	Date the substance or the mixture was last supplied by that supplier	Ten years
	Regulation (EU) No 305/2011	Technical documentation and declaration of performance on construction products	Date the product was placed on the market	Ten years
8. Other records	Data Protection Act	Personal data of employees in network systems, computer systems, communication equipment used by employees, access controls and other internal management/administration	N/A	To the extent that the correspondence contains personal data, it should not be kept for longer than is necessary for the lawful purposes for which such personal data was processed
	Data Protection Act	Correspondence	N/A	To the extent that the correspondence contains personal data, it should not be kept for longer than is necessary for the lawful purposes for which such personal data was processed
	Data Protection Act	Camera recordings	N/A	There is no specified period in the legislation, but the guidance of the Information Commissioner's Office confirms that images should not be kept for longer than strictly necessary to meet the organisation's purposes in recording them. On occasion, an organisation may need to retain images for a longer period where a law enforcement body is investigating a crime.

9. Emails stored on Exchange Server, Enterprise Vault, locally to user and backups	Data Retention (EC Directive) Regulations 2009 (note these have been repealed – however there is a lack of clarity in this area)	Legal	Date of communication	As long as is necessary
	Data Retention (EC Directive) Regulations 2009 (see comment above)	Financial	Date of communication	As long as is necessary
	Limitation Act	HR (employees)	Date employment ceases	6 years (potential wrongful dismissal/breach of contract claim)
	Equality Act 2010	HR (Unsuccessful Job Applicants)	Date notified unsuccessful	3 months (potential discrimination claim)
10. Telephone calls	Data Retention (EC Directive) Regulations 2009 (see comment above)	Legal	Date of communication	As long as is necessary
	Data Retention (EC Directive) Regulations 2009 (see comment above)	Financial	Date of communication	As long as is necessary
	Limitation Act	HR (employees)	Date employment ceases	6 years (potential wrongful dismissal/breach of contract claim)
	Equality Act 2010	HR (Unsuccessful Job Applicants)	Date notified unsuccessful	3 months (potential discrimination claim)
11. Instant messenger records	Retention of Communications Data under Part 11: Anti-Terrorism, Crime and Security Act 2001, Home Office	HR	Date of communication	As long as is necessary
12. Internal investigation records	Limitation Act	HR Internal Investigation Records	Date employment ceases	6 years
13. Mergers and Acquisitions documentation	Limitation Act	Documentation relating to merger or acquisition of a company	Date of execution of the SPA/Asset acquisition agreement	12 years (most SP/Asset Purchases are concluded as deeds)

14. Criminal records	DBS guidance for employers: Duration of criminal record check validity ICO Employment Practices Code Nov 2011, part 1.7.4	Criminal records requirement assessments for a particular post	Date the assessment was last used	12 months
		Criminal records information forms. Disclosure and Barring Service (DBS) check forms DBS certificates	Date the check has been completed and the outcome recorded (i.e. whether satisfactory or not)	As soon as practicable, or six months if clearly relevant to the ongoing employment relationship
15. Credit checks	Money Laundering Regulations 2007 Limitation Act	Customer Credit checks & credit records	Date which business relationship ends; or when the occasional transaction is completed (AML) Date of last transaction (fraud)	5 years 6 years
15. Working Time Regulations	Working Time Regulations 1998, SI 1998/1833, reg 9	Records relating to and/or showing compliance with Working Time Regulations 1998 including: - registration of work and rest periods - working time opt-out forms	Date on which record was made	2 years
16. National Minimum Wage	National Minimum Wage Regulations 2015, SI 2015/621, reg 59	Records demonstrating compliance with national minimum wage requirements	Date on which the pay reference period immediately following that to which they relate ends	3 years

17. IP address & cookies	S2 and s32 Limitation Act	IP address & cookies		6 years (related to fraud committed by an individual through a specific IP address and any related Cookies)
18. PCI	S 9.4.4.C Payment Card Industry Data Security Standard- Nov 2013	Access visitor logs		3 months
	S 10.7.A Payment Card Industry Data Security Standard Nov - 2013	Audit history log		12 months
19. Sensitive personal data	Data Protection Act	Consents for the processing of personal data and sensitive personal data	Date that data stopped being processed	For as long as the data is being processed and up to 6 years afterwards
20. Sales and Marketing	Privacy and Electronic Communications (EC Directive) Regulations 2003	Consents for certain types of direct marketing	When listed on an active marketing list. Such list should include a list of those who have provided a "GDPR "consent and cross refer to the record of consent.	For as long as consent is not withdrawn.
	Privacy and Electronic Communications (EC Directive) Regulations 2003	Requests to be removed from marketing lists and exception lists	N/A	Until person has been removed.
	Limitation Act 1980	Standard terms and conditions	From acceptance date	Six years
21. General		Email Records (except (i) where the emails are relevant to current or threatened litigation or relate to employment issues in which case they should be printed and kept on the personnel file and retained in accordance with that section or (ii) emails to or from Finance function which should be retained in accordance with retention periods for financial accounts).	From date of email	As long as necessary. The appropriate retention period will depend on the type of information and whether it may be needed for ongoing business purposes or compliance with regulatory requirements.

22. Customer/ Prospect information	Limitation Act 1980	Customer verification documents (e.g. proof of identity or credit references)	From date of collection	On closure of account / when the customer ceases to be a customer
	None	IP addresses and cookies	From collection	Different cookies may be stored for different periods of time
	PCI – DSS requirements and card issuer's instructions regarding minimum data retention periods.	Credit and Debit card transaction details		Minimum of 2 years
	Limitation Act 1980	Customer transaction details and contracts (including contact details where these are relevant to the contractual relationship).	Date of completion of services to customer	6 years from date of completion of services to customer or 12 years if contract was entered into as a deed
	None	Other Personal Data of a Customer ancillary to the contractual relationship	Date ceased to be a customer	Retain whilst current customer, but should normally be deleted within 3 to 6 months of ceasing to be a customer.
23. Customer Payment Methods (PAN- card numbers)	S19 of The Money Laundering Regulations 2007	Customer Payment Methods (PAN- card numbers)	The date: (i) which the business relationships ends, or; (ii) when the occasional transaction is completed	5 years

ABBREVIATIONS

Data Protection Act	Data Protection Act 1998 / 2018 (*The EU General Data Protection Regulation (GDPR) will come into force on 25 May 2018 and the Data Protection Act 1998 will be replaced by the Data Protection Act 2018)
Taxes Management Act	Taxes Management Act 1970
HMRC	Her Majesty's Revenue and Customs
Employers' Liability Regulations 1998	Employers' Liability (Compulsory Insurance) Regulations 1998
Control of Asbestos at work Regulations	Control of Asbestos at work Regulations 2006
Limitation Act	Limitation Act 1980
Companies Act	Companies Act 1985 and 2006
Pensions Act	Pensions Act 1995
The Control of Lead at Work Regulations	The Control of Lead at Work Regulations 2002
The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995
The Statutory Maternity Pay Regulations	The Statutory Maternity Pay Regulations 2006
The Statutory Sick Pay (General) Regulations	The Statutory Sick Pay (General) Regulations 1882 and 2006
Employers' Liability Regulations	Employers' Liability Regulations 1998
VAT ACT	VAT ACT 1994
The Income Tax (Employments) Regulations	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)	The Retirement Benefits Schemes (Information Powers) Regulations

Version Control

This information will be updated annually.

Document:	Department:	Approved By:
Global Data Retention and Disposal Policy	Global Risk & Compliance	General Counsel
Policy Number:	**Policy Last Revised Date:**	**Policy Revision Number:**
	23/03/2019	1
Effective Date:	**Last Review Date:**	**Reviewed By:**
23/07/2019	21/07/2019	Global Director of Risk & Compliance

Summary of Changes

Any approved changes will be made to the document and then added to this table.

Date	Summary of Changes Made	Made By
23/03/2019	Initial Document Modification from Lewis Silkin, LLP Template	Vanessa van Balkom