

# Data Protection Policy

## Contents

1. About this policy.....	2
2. Scope of policy.....	2
3. Guiding principles .....	3
4. Role and responsibilities.....	3
5. Types of data and data classifications.....	4
6. Retention periods.....	5
7. Storage, back-up and disposal of data.....	6
8. Special circumstances.....	7
9. Where to go for advice and questions.....	7
10. Breach reporting and audit.....	8
11. Other relevant policies.....	8

## Annex

### Contents

1. Annex A Definitions.....	9
2. Annex B retention schedule.....	10

## 1. About this policy

- 1.1 The corporate information, records and data of **Apex Resources Limited** (Apex) is important to how we conduct business and manage employees.
- 1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.
- 1.3 This Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.
- 1.4 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.
- 1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

## 2. Scope of policy

- 2.1 This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".
- 2.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices.
- 2.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

### 3. Guiding principles

3.1 Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We regularly monitor and audit compliance with this policy and update this policy when required.

### 4. Roles and responsibilities

4.1 **Responsibility of all employees.** We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All employees must comply with this policy, the Record Retention Schedule, any communications suspending data disposal and any specific instructions from the relevant department and Legal Department. Failure to do so may subject us, our employees, and contractors to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

4.2 The Records Management Department or other designated department that we may establish from time to time are responsible for identifying the data that we must or should retain, and determining, in collaboration with the Legal Department, the proper period of retention. It also arranges for the proper storage and retrieval of data,

co-ordinating with outside vendors where appropriate. Additionally, the Records Management Department or other designated department that we may establish handles the destruction of records whose retention period has expired.

4.3 The Records Management Officer reports to the Records Management Heads. Head of the Records Management Department is responsible for:

- Administering the data management programme;
- Helping department heads implement the data management programme and related best practices;
- Planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and
- Providing guidance, training, monitoring and updating in relation to this policy.

4.4 **Data Protection Officer.** Our Data Protection Officer (DPO) or designated member of staff responsible for data protection is responsible for advising on and monitoring our compliance with data protection laws which regulate personal data. Our DPO works with our Records Management Department on the retention requirements for personal data and on monitoring compliance with this policy in relation to personal data.

## 5. Types of data and data classifications

5.1 **Formal or official records.** Certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see paragraph 6.1 below for more information on retention periods for this type of data.

5.2 **Disposable information.** Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of **Apex** and retained primarily for reference purposes.
- Spam and junk mail.

Please see paragraph 6.2 below for more information on how to determine retention periods for this type of data.

5.3 **Personal data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). See paragraph 6.2 below for more information on this.

5.4 **Confidential information belonging to others.** Any confidential information that an employee may have obtained from a source outside of Apex, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet. Please see our Privacy Policy

5.5 **Data classifications.** Some of our data is more confidential than other data. Our Data Classification Standard explains how we classify data and how each type of data should be marked and protected. When complying with this policy, it is also important that you follow our Data Classification Standard.

## 6. Retention period

6.1 **Formal or official records.** Any data that is part of any of the categories listed in the Record Retention Schedule contained in the Annex to this policy, must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or notice to preserve documents for contemplated litigation or other

special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Records Management Officer or the Legal Department.

6.2 **Disposable information.** The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

6.3 **Personal data.** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data. More information can be found in in our Privacy Policy.

6.4 **What to do if data is not listed in the Record Retention Schedule.** If data is not listed in the Record Retention Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Record Retention Schedule, or if you are unsure, please contact the Records Management Department.

## 7. **Storage, Back-up and disposal of data**

7.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

7.2 **Destruction.** Our Records Management Officer is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be coordinated with the IT Support Team.

7.3 The destruction of data must stop immediately upon notification from the Legal Department that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). Destruction may begin again once the Legal Department lifts the requirement for preservation.

## 8. Special circumstances

8.1 **Preservation of documents for contemplated litigation and other special situations.** We require all employees to comply fully with our Record Retention Schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the Legal Department informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the Legal Department determines those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

8.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Legal Department.

8.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

## 9. Where to go for advice and questions

9.1 **Questions about the policy.** Any questions about retention periods relevant to your function or department should be raised with your function or department data retention lead. Any questions about this policy should be referred to John da Rocha on 01923 200 111; john@apexltd.co.uk who is in charge of administering, enforcing and updating this policy.

## 10. Breach reporting and audit

- 10.1 **Reporting policy breaches.** We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depends largely on employees. If you feel that you or someone else may have breached this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with the Records Management Officer **OR** manager at the next level above your direct supervisor. If employees do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.
- 10.2 No one will be subject to and we do not allow, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.
- 10.3 **Audits.** Our General Counsel and the Records Management Officer will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice to ensure we are in compliance with relevant new or amended laws, regulations or guidance). Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

## 11. Other relevant policies

- 11.1 This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our:
- IT and communications systems policy.
  - IT acceptable use policy.
  - Privacy standard **OR** Data protection policy.
  - Confidentiality policy.
  - Data classification policy.
  - Business continuity policy.
  - And other IT, security and data related policies, which are available on the intranet.



## 1. Annex A

### *Definitions*

**Data:** all data that we hold or have control over and therefore to which this policy applies. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

**Data Protection Officer:** our Data Protection Officer who is responsible for advising on and monitoring compliance with data protection laws.

**Data Retention Policy:** this policy, which explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

**Disposable information:** disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule.

**Formal or official record:** certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

**Non-personal data:** data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised.

**Personal data:** any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data such as health data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

**Records Management Department:** the department responsible for identifying the data that we must or should retain, and determining, in collaboration with the Legal Department the proper period of retention. It also arranges for the proper storage and retrieval of data, coordinating with outside vendors where appropriate and handles the destruction of [some] records whose retention period has expired.

**Records Management Officer:** the Records Management Officer is responsible for administering the data management programme, helping department heads implement it and related best practices, planning, developing, and prescribing data disposal policies, systems, standards, and procedures and providing guidance, training, monitoring and updating in relation to this policy.

**Record Retention Schedule:** the schedule attached to this policy which sets out retention periods for our formal or official records.

**Storage limitation principle:** data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed. This is referred to in the GDPR as the principle of storage limitation.

## 2. Annex B

### *Record retention schedule*

Apex establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

Employees should comply with the retention periods listed in the record retention schedule below, in accordance with the Apex Data Retention Policy.

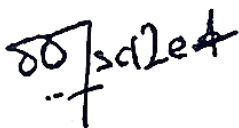
If you hold data not listed below, please refer to the Apex Data Retention Policy. If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this record retention schedule, please contact John da Rocha on 01923 200 111; [john@apexltd.co.uk](mailto:john@apexltd.co.uk)

TYPE OF DATA	RETENTION PERIOD	REASON / COMMENTS
<b>OVERARCHING CATEGORY: Recruitment records OR Payroll records OR Corporate records OR Supplier contracts</b>		
Application forms <b>OR</b> Expenses claims <b>OR</b> Board minutes <b>OR</b> Signed contracts.	A minimum of six years and a maximum of 10 years.	To be added on a case by case basis.

**Contact Us**

Head Office: **Apex Resources Ltd**  
**Apex House**  
**1 Bridle Path**  
**Watford**  
**Hertfordshire**  
**WD17 1UE**

Tel: **01923 200111**  
 Fax: **01923 200112**  
 Email: [info@apexltd.co.uk](mailto:info@apexltd.co.uk)  
 Web: [www.apexltd.co.uk](http://www.apexltd.co.uk)

Signed: 

Date: 02/12/2024

Tope Osazee, Managing Director