GRAVITY | PRIVATE WEALTH

Record Keeping Policy

File Information

Responsible Unit	Date of issue	Publication No
Regulatory Compliance & AML	01/08/2024	v.1

Archive History

Publication No	Date	Description of Modifications
v.1	01/11/2024	Original Edition

Board of Directors Approval

Board of Directors	Meeting Date

Table of Contents

1. Introduction

Gravity Private Wealth Ltd (hereinafter the "Company") is an Investment Firm incorporated and registered under the laws of the Republic of Cyprus, with registration number HE 442079. The Company is authorized and regulated by the Cyprus Securities and Exchange Commission (“CySEC”) under license number 447/24.

The Company acknowledges the need to establish, implement and maintain effective and transparent policies and procedures for the prompt handling of clients / Company documents and records, which fulfil its operational needs and comply with statutory and regulatory requirements pursuant to the Markets in Financial Instruments Directive (Directive 2014/65/EU) ("MiFID II") and Regulation 2014/600/EU (“MiFIR”), as well as respond to the expectations of its stakeholders.

In this context, the Company establishes an effective Record Keeping Policy (hereinafter the "Policy”) in order to define the framework and provides relevant guidance for the management of its records.The Board of Directors (the “Board”) has the responsibility of establishing this Policy, approving any subsequent amendments / revisions and ensuring that disciplinary measures are taken when the rules of this Policy are violated. In cases where there are references in any of the internal policies and procedures of the Company in relation to issues covered by this Policy, which were approved prior to the approval of this Policy, the provisions of this Policy will prevail.

2. Purpose of this Policy

This Policy aims to provide the required guidance regarding the documents (both in paper and electronic format) retention period, received or created during the provision of Investment Services to clients, as well as to establish a framework in order for the employees of the Company to clearly understand their responsibilities in relation to the requirements imposed by MiFID II with regards to the documentation, storage and retention period of certain Records. This Policy also provides guidelines on how long certain documents should be retained.

The provisions of this Policy apply at all times, unless:

- the Records under question are or could be subject to the future litigation;
- there is a dispute that could lead to litigation; or
- the Company is a party to a lawsuit; or

- an investigation is conducted by CySEC or any other competent judicial, governmental, supervisory or regulatory body,
- where, such Records must be preserved until the AML and Compliance Officer determines that are no longer needed.

3. Policy Applicability

The Policy applies to:

- All records (both original documents and reproductions) created, received, provided or maintained by the Company's relevant employees;
- All the Company's departments involved in the provision of Investment services; and
- All types of clients and / or counterparties to which the Company provides Investment Services.

All concerned staff members of the Company should be aware of the provisions of this Policy and understand the role and importance for the retention of Records pertaining to the offering of investment services.

The Policy and any subsequent amendments are distributed to and are binding to all employees.

It is the Company's policy to maintain complete, accurate and high-quality records. Records are to be retained for the period set forth in "Record Retention Schedule" section of this document, unless longer retention is required for historical reference, contractual, legal or regulatory requirements or for any other purpose.

No employee or director of the Company shall knowingly destroy information or a document with the intention to obstruct or influence the investigation or proper administration of any matter within the Company's departments.

It is noted that records is defined as the following information / documentation, but not limited to: legal documentation, client data / statements, electronic mails, telephone conversations and electronic communications (e.g. instant messages (e.g. Bloomberg / Reuters), minutes of face-to-face meetings, telephone recordings), electronic documents (e.g. Microsoft Office Suite and PDF files) or other formatted files, regardless of the format or media (paper, electronic or other format), preserved about facts, events or transactions which are created or received by or on behalf of the Company for providing its investment services / activities.

4. Regulatory Framework

The Policy has been prepared in accordance with the following laws, regulations, directives and guidelines:

- Cyprus Law 87(I)/2017, as amended and in force, titled "Provision of Investment Services, Exercise of Investment Activities, Operation of Regulated Markets and Other Related Matters" (hereinafter the "MiFID II Law"),
- Regulation (EU) No. 600/2014 of the European Parliament and of the Council, of 15 May 2014 on Markets in Financial Instruments;
- Commission Delegated Regulation (EU) No. 2017/565 of 25 April 2016, supplementing EU Directive 2014/65 titled "On market in financial instruments" (hereinafter the "MiFID II"),
- EU Directive 2014/65 titled "On market in financial instruments" (hereinafter the "MiFID II");
- CySEC Circular 251 titled "ESMA Guidelines on transaction reporting, order record keeping and clock synchronisation under MiFID II" (hereinafter the "C251"),
- Law 125(I) of 2018 Providing For The Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of Such Data, implementing the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR').
- Other laws, directives and circulars issued by the European Securities and Markets Authority ("ESMA") and the Cyprus Securities and Exchange Commission ("CySEC") from time to time, applicable to this Policy.

5. Roles and responsibilities

The Company's Board has the responsibility, amongst others, to ensure:

- the overall implementation of the Policy;
- that the Policy is effectively communicated to all directors and employees of the Company;
- compliance with the provisions stipulated in the Policy;
- the timely and effective training and education of the concerned employees;
- that disciplinary measures are taken and enforced when rules are not followed by employees; and
- the approval of the present Policy, as well as any subsequent amendments/revisions made.

The Senior Management have the responsibility of:

- ensuring that an organizational structure/ arrangement is in place securing the effective implementation of the provisions of this Policy;

- exercising effective oversight over the Company's document retention related arrangements and controls;
- undertaking training and education in connection with this Policy; and
- ensuring that disciplinary measures are taken and enforced when rules are not observed by employees.

The Regulatory and Compliance Department has the responsibility to:

- ensure that the provisions stipulated in this Policy are followed at all times;
- periodically evaluate the effectiveness of the Policy and adopt any alternative or additional measures as are necessary and appropriate
- periodically review and check whether the Records are kept for the appropriate period of time;
- providing advice in relation to the implementation of this Policy; and
- make available the above information to the relevant Competent Authority, if requested.

The IT Department has the responsibility to:

- oversee the development and periodic review of document retention arrangements in order to ensure compliance with its relevant obligations;
- ensure that all means of Records are properly stored, readily accessible, are of good quality and have not been altered;
- monitor on an on-going basis the Company's compliance in relation to the IT provisions stipulated in this Policy.

The internal Audit Department has the responsibility to perform an audit, at least of an annual basis, in order to assess the compliance level of the employees/departments, as well as the Company as a whole, in connection with the provisions stipulated in this Policy.

6. Types of Records

In the context of its business scope, the Company is required to keep the following business records and records related to its fiduciary obligations:

- Journals and other records forming the basis of entries in any ledgers.
- General ledger reflecting assets, liabilities, capital, reserves, income and expenses.
- Accounts, books, working papers and other records substantiating prior performance claims
- Memorandum/audit log of each order placed on behalf of a client.
- Bank records, including check books, bank statements, canceled checks and cash reconciliations.

- Bills and statements.
- Trial balances, financial statements and internal audit working papers.
- Copies of proxy voting policies.
- Journals showing securities transactions.
- Corporate formation and governance documents.
- Copies of documents used in making a decision as to how to vote proxies.

The Company shall provide clients, or potential clients, in good time and before the provision of investment services with, but not limited to, information / documentation described below.

Information to clients

General Information:

- Records of sale and purchase transactions and access to a client's current securities position.
- Copies of trade confirmations and the order received from clients for execution.
- Information regarding each order received from a Client or decision taken to deal as well as executed orders (i.e. transactions following the order processing).
- Record for each security held by client showing amount and location.
- Copies of proxy statements received regarding client securities.
- Records of votes cast by the Company on behalf of client, as the case may be.
- Copies of client correspondence requesting how the adviser voted proxies.
- List of client accounts in which the Company has discretionary authority and instruments granting discretionary power (powers of attorney).

Information concerning Client Categorisation, Appropriateness, Target Market Assessment and Investment advice:

- Client Categorisation/ Re-categorisation letters;
- Client Consent letters/ Warning letters;
- Client Quesitionnaire;
- Records regarding the appropriateness /suitability assessments performed by the Company /results of the appropriateness /suitability assessments ensuring that arrangements are designed to enable the detection of failures regarding the suitability assessment (such as mis-selling). Regarding the suitability assessment, relevant information about the client should be recorded (including how that information is used and interpreted to define the client's risk profile), and information about financial instruments recommended to the client or purchased on the client's behalf. Specifically:

  - any changes made by the Company regarding the suitability assessment, in particular any change to the client's investment risk profile;
  - the types of financial instruments that fit that profile and the rationale for such an assessment, as well as any changes and the reasons for them.
- Record regarding any investment advice provided and all investments (and disinvestments) made;
- Warning letters given to clients in cases where the Investment Service or product was assessed as non-appropriate for the Client;
- Warning letters given to clients in cases where the Client did not provide sufficient information to enable the Company to undertake a proper appropriateness assessment;
- Target market assessment related documentation (e.g. European MiFID Template);
- Other Client informative related documentation (e.g. license, financial statements, KYC related documents).

Information on costs and charges:

- Information about all costs and charges related to both the financial instrument (s) and Investment / Ancilliary Service(s) provided to the Company's clients;
- Information regarding the itemised breakdown of cost and charges, upon Client's request;
- Illustration showing the cumulative effect of costs on return when providing Investment Services.

Telephone Conversations and Electronic Communication records

- The Company should at least record all telphone conversations and wWritten communications, to and from client relating to the execution, reception and transmission of Client orders, in line with the provisions stipulated in the Company's Internal Operations Manual.

Marketing communication:

- All marketing communication related information that the Company disseminates in such a way that is likely to be received by clients or potential clients.

Written agreements with clients

All client agreements, which set out the respective rights and obligation of the Company and the client, irrespective of the Client categorization, should be stored at least during the period of the client relationship. Client agreements related documentation should include, among others, the following:

- Terms and Conditions;
- Order execution policy;

- Risk disclosure statement;
- Conflict of interest policy;
- Client categorization notice;
- Complaints handling procedure;
- Privacy policy;
- Key Information Documents;
- Any other Agreeement signed between the two parties.

Information relating to the safeguarding of client financial instruments or client funds and use of client financial instruments

- Statements of Client Financial Instruments and /or Client funds (Specimen of Account Statement);
- Safeguarding of periodic reports to clients;
- Periodic reviews of Custodians, including due diligence reviews;
- Reconciliations performed by the Company in relation to Client funds and / or Financial Instruments against custodian statements;
- Client consent for using Client's Financial Instruments;
- Information to clients in relation to the portfolio management or contingent liability transactions (i.e. statements when the overall value of the portfolio / positions in leveraged financial instruments or contingent liability transactions depreciated more than 10%).

Personal transaction records

- Records of Personal Transactions notified to the Company or identified by it, including any authorisation or prohibition in connection with such a Transaction.
- In the case of Outsourcing arrangements, it should be ensured that the firm(s) to which the activity is outsourced maintains a record of Personal Transacitons entered into by any Relevant person and provides that information to the Company promptly on request.

Client order handling records, record keeping of orders, transactions and order processing

- Order received from clients for execution;
- Records regarding orders executed on behalf of clients or transmitted to a third party (e.g. broker) for execution;
- Trade confirmation reports/ statements;
- Reconciliation of transactions;
- Information regarding each order received from a Client or decision taken to deal as well as executed orders (i.e. transactions following the order processing).

Complaints handling records

The following Records shall be established/ documented and maintained by the Company in relation to Complaints handling requirements:

- "Client Complaint Form" received from clients or potential clients;
- Complaints Register for recording clients' complaints;
- Documentation related to the reporting of clients' Complaints to CySEC; and
  Other related documentation (e.g. letters to clients, documentation of Complaints' internal assessment).

Regulatory/ Internal related reports/ documents

This sub-section describes all reports that demonstrate the Company's Compliance with the applicable regulatory framework governing the Investment and/ or Ancilliary Services/ Activites offered to its clients. Such reports/ documents are prepared, maintained and communicated to the Company's Senior Executive Management, the Board as well as the Competent Authority.

Such reports/ documents include, among others, the following:

- Compliance/ Risk Management/ Internal Audit reports submitted to the Company's Board on the implementation and effectivenenss of the overall control environment for Investment Services and Activities, on the risks that have been identified and on the complaints-handling reporting as well as remedies undertaken or to be undertaken;
- Conflicts of Interest register;
- Records regarding personal transactions;
- Other Records required by MIFID II / the Law and described in the Company's Regulatory Compliance Policy.

Policies and procedures

- The Company should keep records in a sufficient way in order to enable the Competent Authority to fuflil its supervisory tasks and to perform the enforcement actions under MIFID II and Market Abuse Regulation (MAR), and in particular to ascertain that the Company has complied with all relevant obligations, including those with respect to clients or potential clients and to the integrity of the market.
- In this respect, the Company shall maintain all the policies, procedures as well as other relevant documents (e.g. departmental procedures, transactions) in relation to MIFID II and MAR.

Telephone Conversations and Electronic Communication records

The Company should at least record all telphone conversations and written communications, to and from client relating to the execution, reception and transmission of Client orders in line with the provisions stipulated in the Company's Internal Operations Manual.

7. Retention Period Schedule

Nature of obligation	Type of Record	Retention Period
Client assesment		
	Information to clients	• Duration of Client relationship; and • Five (5) years after its termination
	Client agreements	• Duration of Client relationship; and • Five (5) years after its termination
	Appropriateness assessment	• Five (5) years, 7 years if requested by CySEC.
Order handling		
	Client order handling-aggregated transacitons	• Five (5) years, 7 years if requested by CySEC
	Aggregation and allocation of transactions for own account	• Five (5) years, 7 years if requested by CySEC
Client Orders and transactions		
	Record Keeping of client orders	• Five (5) years, 7 years if requested by CySEC

Prompt fair and expeditious execution of client orders and publication of unexecuted client limit orders for shares traded on a trading volume	Record Keeping of transactions and order processing	• Five (5) years, 7 years if requested by CySEC
Reporting to Clients		
	Obligation in respect of services provided to clients	• Duration of Client relationship; and • Five (5) years after its termination.
Safeguarding of Client assets		
	Client financial instruments held by an investment firm	• Duration of Client relationship; and • Five (5) years after its termination.
	Client funds held by an investment firm	• Duration of Client relationship; and • Five (5) years after its termination.
	Use of client financial instruments	• Duration of Client relationship; and • Five (5) years after its termination.
Communication with Clients		
	Information about Costs and associated charges	• Five (5) years, 7 years if requested by CySEC
	Informaton about the investment firm and its services, financial instruments and safeguarding of client assets	• Five (5) years, 7 years if requested by CySEC
	Information to clients	• Five (5) years, 7 years if requested by CySEC
	Marketing communication (except in oral form)	• Five (5) years, 7 years if requested by CySEC

	Telephone Conversations and Electronic Communications recordings	• Five (5) years, 7 years if requested by CySEC
Organisational requirements		
	The firm's business and internal organisation	• Five (5) years, 7 years if requested by CySEC
	Compliance reports	• Five (5) years, 7 years if requested by CySEC
	Conflict of Interest record	Five (5) years, 7 years if requested by CySEC
	Risk Management reports	• Five (5) years, 7 years if requested by CySEC
	Internal Audit reports	• Five (5) years, 7 years if requested by CySEC
	Complaints-handling Records	• Five (5) years, 7 years if requested by CySEC
	Records of personal transactions	• Five (5) years, 7 years if requested by CySEC

8. Record Keeping Standards

Pursuant to MIFID II, the Company should establish and implement adequate arrangement and mechanisms in order to ensure that Records regarding:

- Investment Services / Activities provided by the Company to its clients / counterparties; and
- transactions concluded between the Company and its clients / counterparties, are adequately stored and maintained for the required retention period.

Records must have relevant content, context and format, and must be accurate, authentic, useable, reliable, timely and well managed. They must be retained in a format that does not allow them to be altered or deleted.

The records shall be retained in a medium that it allows the storage of information in a way accessible for future reference and in such a form and manner that the following conditions are met:

- the Competent Authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;
- it is possible for any corrections or other amendments and the content of the Records, prior to such corrections or amendments, to be easily ascertained;
- it is not possible for the records otherwise to be manipulated or altered;
- it allows the Head of Information Technology or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and
- the Company's arrangements comply with the record keeping requirements irrespective of the technology used and are adequate to mitigate any shortcomings or limitations of the record-keeping arrangements.

Further to the records described in this Policy, the Company is also obliged to keep all policies and procedures required by MiFID II, the Markets in Financial Instruments Regulation (EU) No 600/2014, the Regulation (EU) No 596/2014 on market abuse ("MAR") as well as the Directive 2014/57/EU on criminal sanctions for market abuse ("CSMAD"), in order to ascertain that the Company has complied with the relevant obligations.

It is also noted that the Competent Authority may require the Company to keep additional records to those identified in this Policy.

In addition, the following are noted:

- Records must directly relate to and support a service, function or activity delivered by the Company, and be able to support decision-making.
- Records must serve the interests of the Company, its staff and other stakeholders by maintaining high quality documentation for appropriate lengths oftime.
- Records must be managed via systems and processes ensuring efficiency and consistency throughout their lifecycle of creation, distribution, use, maintenance and disposition.
- Records must be managed and stored in a suitable format to retain quality, relevance, accessibility, durability and reliability. Any transfer to another format must have due regard to retaining these qualities.
- Records must be kept securely as befits the confidentiality and importance of the content, being protected from unauthorised or unlawful disclosure.
- Records must be accessible and retrievable as required to support business efficiency and continuity.
- Records must be retained or disposed of in compliance with the Policy.

- Records must be subject to clearly defined arrangements for appraisal to select those worthy of permanent preservation.
- Records must undergo appropriate destruction when no longer required, in an organised, efficient, timely and (where necessary) confidential manner.

9. Retention, Safety and Management of Records

The principle around records retention is to ensure that records are maintained properly and in line with the provisions of MiFID II throughout their lifecycle. In particular, a record's lifecycle consists of the following stages:

1. Creating records;
2. Organising records: Use and maintenance;
3. Storage and Retention;
4. Security and Access;
5. Retrieving records;
6. Disposing records.

Creating records

Each function of the Company must have in place adequate systems for documenting its principal activities, including information received from clients/ counterparties in different forms or format, such as written form, electronic form, etc. Each concerned department should create and maintain records that serve its functions and the standards detailed above. The records must be accurate and complete, including all investment services offered as well as transactions undertaken with its clients/ counterparties, so that it is possible to establish what has been done and why. The quality of the records must be sufficient to allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met. The integrity of the information contained in records must be beyond doubt; it should be compiled at the time of the activities to which it relates, or as soon as possible afterwards, and be protected from unauthorised alteration or deletion.

Where appropriate, templates should be used, so that documents are produced consistently and quickly. In addition, version control procedures are required for the drafting and revision of documents, so that staff can easily distinguish between different versions and readily identify the latest copy.

The retention of duplicate records presents enhanced risks regarding their management, use and alteration. Whereas there may be a need to keep local versions of records held centrally, it should be avoided where

possible and a system enabling use of a single central version implemented. File titles should be brief but comprehensible with a consistent format used.

Organising records: Use and maintenance

Records should be organised and described in a uniform, logical manner that facilitates fast, accurate and comprehensive retrieval so that they are easily accessible when required.

Each concerned department is responsible for the maintenance of its own Records and shall maintain and safeguard the integrity of those Records for the required retention period.

A filing structure or records series should be used, i.e. a group or unit of related records, documents or information that is normally filed or kept together because they relate to a particular subject or function, or result from or document a particular activity.

Classifying records and holding them in an appropriate structure or scheme will enable suitable retention periods to be assigned. Keeping diverse records together in a less structured manner makes it more difficult to identify and retrieve them when required, and to apply responsible retention policies.

Standardised referencing and titling must be employed, so that information can be readily identified and retrieved. Naming conventions will assist with using consistent terminology to improve efficiency. Titles given to digital and hard copy records and files should describe the content or subject matter accurately and helpfully.

Off-site storage and retention

Records should be stored in a searchable format in such a medium that ensures theirusability, reliability, authenticity and preservation for a period at least equal to the required retention period.
When storage space for hard-copy records is an issue, the Company uses off-site storage. This can be a cost-effective way of managing records but careful thought should be given to the types of records that are selected for offsite storage, in particular how quickly and frequently such records may need to be accessed. There are additional costs for retrieval of records and there can also be a short delay.

A scanning service is also available which can assist with storage needs and make records more accessible. It can bring significant benefits but careful consideration should be given to whether scanning is a suitable solution, as it can impact on the legal or evidential integrity of documents, and may not be suitable for a series of records to which information is still being added.

Security and access

Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information contained in specific Records (e.g. personal, commercial or operationally sensitive

information). Each of the Company's departments shall liaise with the IT Department and establish / implement the necessary arrangements (e.g. access rights, passswords or system access restrictions) in order to safeguard such information.

For example, electronic Records shall generally be stored in shared drives (with appropriate confidentiality protection) or in case of hard copies, secured/ fireproof cabinets shall be used.

The Company's information classifications scheme has the following five categories of confidentiality which should be used to classify information and records held by the Company. It will assist with determining appropriate practice regarding storage, access, handling and disposal of records.

Classification	Definition
Public	May be viewed by anyone, anywhere in the world
Normal	Available to all authenticated members of staff
Confidential	Available only to authorised and authenticated members of staff
Strictly Confidential	Access is controlled and restricted to a small number of named, authenticated members of staff

An access policy, taking into account the confidentiality of information, should identify who is permitted to have access to which records and to highlight if special security measures are required for any records. Records should not be only accessible by a single person but should be stored in centralised storage or filing systems or on a shared drive, so that departments can operate efficiently when individual members of staff are absent. Where appropriate, access to central records should be appropriately available across the Company in order to avoid recreating information that already exists and storing duplicate data unnecessarily.

Records that would be vital to the continued functioning of the Company in the event of a disaster must be identified and protected. These include records that would recreate the Company's legal and financial status, preserve its rights, and ensure that it continues to fulfil its obligations to its stakeholders. All critical business data must be protected by appropriate preservation, backup and disaster recovery policies. Where vital records are only available in paper format it is best practice that they are duplicated, and the originals and copies stored in separate locations. If, however, duplication is either impracticable or legally unacceptable, fireproof safes should be used to protect vital documents.

Retrieving records

In the event of request of records by Competent Authority and/ or Clients, records shall be retrieved at any point without undue delay. It is therefore essential to be stored in searchable format, allowing the Company to deliver such Records as soon as possible.

Disposing Records

When a record reaches the end of its retention period a decision must be taken on its disposal, with the three possible outcomes:

- Reappraisal
- Permanent preservation / Send to Company's archives
- Destruction

Reappraisal

Before action is taken to permanently preserve or destroy a record at the end of its retention period, a reappraisal of any need to retain it for present functions should be undertaken, but it should only be necessary to attribute a revised retention period on rare occasions. In some circumstances it may be necessary to retain a record for longer than its defined retention period. A new operational function requiring its retention may have arisen, or it may be required for investigation or litigation purposes, or because it is needed to respond to an access request received under data protection or freedom of information legislation. If a record needs to be retained for longer, then a new retention timescale should be assigned to it. It is recommended that this date should not be too far in the future, enabling regular review of the decision while taking circumstances into account. A period of one five years is recommended.

Permanent preservation

Some of the Company's records are retained permanently. The following records are examples of items that may be worthy of permanent preservation:

- Records that document policy formation
- Records that show the development of the Company's infrastructure
- Records that show evidence of important decisions or precedent
- Papers relating to the Company's governance, including agendas, minutes, supporting documents and reports relating to Board and other decision-making bodies.

If electronic records have been identified as having archival value then consideration should be given to whether they are retained in a format deemed to be future proofed, and how they can be transferred and stored for permanent preservation.

Destruction

The AML and Compliance Officer is responsible for ensuring that records are destroyed in a timely, safe and secure manner, and that all employees are aware that the destruction is taking place. All copies, including security copies, preservation copies and where possible backup copies, held in any format must be destroyed at the same time.Destruction must be carried out in a way that takes full account of the confidentiality of the record using the Information Classification Scheme. For hard copy records the following requirements apply:

Classification	Method of disposal
Public	Can be disposed of in ordinary waste or recycling bins.
Open	For some records in this category disposal in ordinary recycling bins will be appropriate, but many must be shredded.
Confidential	Must be shredded.
Confidential & Sensitive	Must be shredded.

When an entire file or archive box is to be destroyed the whole file or box must be destroyed in line with the requirements of the most sensitive documents it contains.

It is very easy for multiple duplicate copies of digital information to exist so when disposing of digital records it is vital that all the various locations that a file could be stored have been considered. These include information that may be stored in:

- Company's shared files
- Cloud suppliers whose services are provided by the Company (e.g. Google Drive, OneDrive), and those that aren't (e.g. Dropbox)
- Emails and email attachments
- Individual devices such as laptops, hard drives and USB sticks, whether Company-owned or personally-owned

Staff with access to digital records that are being deleted should ensure that any copies held anywhere in their email folders, files stores and recycle bin are also deleted to ensure completion. Deletion of an electronic file removes the link to the file but it is possible that the file contents could still be retrieved using technical measures. Consequently, adequate security must continue to be applied to file locations and

devices used to hold them until they have been fully expunged or wiped. System backups will continue to hold copies of deleted digital records until such time that the backup is deleted. Whereas the requirements of the Law technically still apply to such records, the Information Commissioner's Office have taken a pragmatic approach to this type of content, recognising that it is possible to put it 'beyond use' while still held so rendering it out of scope. This will only apply if there is no intention to access or use it again, and it would require disproportionate effort to retrieve.

Records of disposal

For potentially significant information a record should be kept of what has been disposed of, why it was disposed of and who authorised it, covering both destruction and transfer to archive. This will ensure there is a transparent audit trail detailing evidence of records that have been destroyed in line with the Company's stated procedures.

Disposal of IT equipment

All disposal of IT equipment must be conducted via IT support services to ensure that it is done securely and that any information remaining on any storage device is securely wiped.

10. Implementation and Review

The Company acknowledges its responsibility to establish, implement and maintain an effective written Record keeping Policy.
The following circumstances, amongst others, can trigger the review process at an earlier stage:

- Change in the services and product mix of the Company;
- Identification of situations that are not adequately captured in the Policy;
- The applicable legislation requires the update of the Policy.

However, the Company has the right to amend the current Policy at its discretion and at any time it considers suitable and appropriate. Where any amendments take place, the updated version of the present Policy shall be distributed to the Company's Employees who shall acknowledge that they have read and understood the updates.

Any amendment or revocation of this Policy shall be approved by the Board.

The Regulatory Compliance Department will use all reasonable endeavours to ensure that the Policy remains current and applicable to the existing business as well as any new business of the Company. The Regulatory Compliance Department will also make sure that the Policy remains appropriate to the structure and size of the Company as well as the nature, scale and complexity of the Company's business model.

11. Policy Violations

Where an allegation is made to the effect that an employee has violated this Policy, whether or not this is intentional, the matter shall be dealt with under the Company's internal rules. Where, after an internal investigation and subsequent disciplinary hearing, the allegation is upheld, the employee will be subject to a disciplinary action / penalty, which can include termination of employment.

Remedial and / or disciplinary action (where applicable) against employees and members of management and third parties may also include reimbursement or litigation, depending on the severity of the incident.