Record Keeping Policy

Policy Overview

The Financial Conduct Authority (FCA) expects firms to conduct their business within the Principles for Business and Consumer Outcomes they have put in place.

To ensure that these principles and consumer outcomes are met, the FCA has set out specific rules and guidance around record keeping, these can be found in the FCA Handbook. The GDPR also sets out rules in relation to how a business can keep records.

Network Members of ITC Compliance should ensure that records are kept in line with the GDPR and the FCA rules and any records disposed of are done so securely. This policy will provide guidelines regarding responsibilities for record keeping.

Who is Responsible for This?

Network Members are required by law and the FCA to adhere to the rules set out in the GDPR and the FCA Handbook and to have stringent processes in place to ensure this.

How does this Affect You?

Definitions

Record	The International Organisation for Standardisation (ISO) defines a record as information that has been created, received and maintained as evidence and information by an organisation or person in the pursuance of legal obligations or in the transaction of business.
Essential Records	Essential records contain information that the business cannot operate without; the information is either irreplaceable or difficult to replace and will typically contain some confidential information.
Confidential Records	Confidential records contain privileged or non-public information pertaining to the company's business, which may relate to internal matters e.g. strategic and operational plans, staff remuneration, etc. as well as dealings with customers and third parties, such as insurers, agents, regulators, etc.

Examples of items that are deemed to be records include;

- documents (including written and typed documents and annotated copies);
- paper based files (i.e. sales/customer and non-insurance transaction files);
- computer files (including word processed documents, databases and presentations);
- emails;
- diaries;
- faxes;
- brochures and reports;
- intranet and internet web pages;
- forms and applications;
- audio and video tapes, including CCTV;
- photographs.

A Network Members management team is responsible for ensuring records are properly retained and disposed of in accordance with the firm's legal obligations. If paper and computer-based records are

used, care needs to be taken in the design of record keeping arrangements and the protection of records.

Retention of Records

Information should be retained within structured record keeping systems, which may include documents as well as information in electronic format.

Records must be retained in an appropriate manner and should be easily retrievable, therefore;

- documents contained in both paper and electronic files should be stored in a logical manner that allows ease of access and retrieval of records. Customer, agency and non-insurance transaction files should be segregated by transaction stages or events; e.g. quotations, responses to queries, application form, etc.
- call recordings should be clear and capable of being transcribed;
- amendments or corrections following a transaction or event must be clearly shown as such and the original information remains visible;
- it should not be possible for details of transactions or events in paper files i.e. sales/customer, agency and non-insurance transaction files (including referencing records) to be manipulated or altered without a record of the change being captured so as to avoid the potential for fraud;
- it should be possible for records in other languages to be reproduced in English;
- any records of consent obtained from or instructions given by employees, customers, suppliers or any other third parties regarding the use of personal, sensitive or confidential data should be retained securely.

The degree of security required around accessibility and storage should reflect the sensitivity and confidential nature of any information recorded.

Retention Periods

The schedule below details minimum retention periods for a range of categories, which have statutory requirements for record keeping/retention periods.

Some records will be retained by ITC Compliance and some by the Network Member.

Record category	Retention period
Company information	Incorporation documents – Permanently Statutory returns – Permanently Register of Members – Permanently Pension schemes records - Permanently Banking records – 6 years Charities and Political Donations -12 years
Corporate Governance	Permanently
Property documents	Deeds of Title – until sold or transferred Leases – 12 years from termination Agreements with architects and builders - 6 years after completion
Human Resources	Job application and interview records – 6 months after notifying unsuccessful candidate

	Personnel and training records – 6 years after employment ceases Payroll records (including maternity, sick pay) 6 years Health and Safety records – all notifiable accidents, dangerous occurrences, reportable diseases – 6 years after employment ceases.
Tax documents	6 years
Contracts	Contracts under seal - 12 years after expiry of contractual obligations Other contracts (i.e. insurer contracts, delegated authority agreements) - 6 years after expiry of contractual obligations Trust deeds - Permanently
Insurance business	Public liability, Product liability and Employer's liability policies - Permanently Other policies – 2 years following policy lapse or until claims under the policy are barred (whichever is the longer). Cancelled or lapsed policies – 2 years from cancellation or policy lapse date Complaints – 3 years from the date the complaint was received (DISP 1.9.1) ITC Compliance will retain records longer than the minimum standards stated above
Intellectual Property Records	Certificates of Registration of trade/service marks – 6 years after cessation of registration Intellectual property agreements and licenses – 12 years after expiring
Property	Documents under seal – 12 years after expiring Other contract - Current year plus 6 years Trust Deeds - Permanently
Supplier agreements	Contracts for products with suppliers – 10 years after the contract was terminated or product no longer used, whichever is the latter

Paper & Electronic Records

ITC Compliance, Network Members and the respective management teams should ensure paper and electronic records (especially those that contain confidential information; e.g. personal details of customers or the company's business plans etc.) held on office premises are kept secure and; access is restricted to staff members authorised to use such information; paper records are placed in lockable cupboards or if necessary, in fire resistant cabinets; and if essential for the running of the business, such records are retrievable in a reasonable timeframe in accordance with the Business Continuity Plan.

Disposal of Records

All information of a confidential or sensitive nature held on paper or in electronic format should be securely destroyed when no longer required.

This is a requirement under GDPR and an expectation of the FCA. The disposal of records, in any format, should be conducted with utmost care and diligence and the confidentiality rights of employees, customers and third parties should be considered.

Safe and Secure Disposal of Records

When disposing of records (in whatever media – paper or electronic) either on or off-site, after the expiry of the retention period, it is important to use a secure method which does not allow future use or reconstruction of information by unauthorised individuals.

When outsourcing destruction to a third party a destruction certificate should be obtained and subsequently retained in a secure place to evidence that the proper process has been followed to carry out the destruction.

Disposal of Paper Records

Paper records containing confidential and/or personal information should be cross-cut shredded and disposed of through reputable waste collection companies. Under no circumstances should confidential and/or personal information be disposed of with other rubbish or general papers.

Electronic Records

Special care should be taken with electronic records, which can be reconstructed from deleted information if the data has not been erased thoroughly. The deletion of electronic records ultimately means the complete destruction of the electronic record and should be organised in conjunction with the firm's IT Department.

Simply erasing or reformatting computer disks or personal computers with hard drives, which once contained personal information, is not enough.

Monitoring & Reporting

Network Members are responsible for ensuring adequate processes are in place for checking that records are maintained adequately, are accurate, not excessive, archived when appropriate and not held for longer than is necessary.

Management Information

ITC Compliance and Network Members should maintain robust processes on record keeping, reviewing them periodically to ensure that compliance is maintained.

Key Points to Remember

Key Point	Notes
GDPR	Network Members are required by law to adhere to the rules set out in the GDPR in regard to record keeping
Record	The International Organisation for Standardisation (ISO) defines a record as information that has been created, received and maintained as evidence and information by an organisation or person in the pursuance of legal obligations or in the transaction of business.
Essential Record	Essential records contain information that the business cannot operate without; the information is either irreplaceable or difficult to replace and will typically contain some confidential information.
Confidential Records	Confidential records contain privileged or non-public information pertaining to the company's business, which may relate to internal matters e.g. strategic and operational plans, staff remuneration, etc. as well as dealings with customers and third parties, such as insurers, agents, regulators, etc.
Example of Records	Examples of items that are deemed as records include; • documents (including written and typed documents and annotated copies); • paper based files (i.e. customer and non-insurance transaction files); • computer files (including word processed documents, databases and presentations); • emails; • diaries; • faxes; • brochures and reports; • intranet and internet web pages; • forms and applications; • audio and video tapes, including CCTV; • photographs.

Date of issue	Version	Brief Description of Change (e.g. sections altered and reasons)
31/01/2023	v3.0	Content updated – CRO
22/02/2023	v4.0	Layout/formatting corrections
23/02/2024	v5.0	Annual review. No change