THE PROMISE SCOTLAND LIMITED

DATA RETENTION POLICY

IMPORTANT NOTICE

This policy applies to staff of The Promise Scotland Limited in the course of their work. It is extremely important that you read this policy and comply with it. This policy will be updated and amended from time to time. You will be notified of changes and a copy will be made available on Sharepoint.

Revision history:

Version	Date	Amended by	Summary of Changes
v1	19/08/21	Z.Iqbal	

ABOUT THIS POLICY

1.1 The corporate information, records and data of The Promise Scotland Limited ("The Promise Scotland", "we" or "us") 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 and Schedule 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:

3.1.1 We comply with legal and regulatory requirements to retain data.

3.1.2 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).

3.1.3 We handle, store and dispose of data responsibly and securely.

3.1.4 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.

3.1.5 We allocate appropriate resources, roles and responsibilities to data retention.

3.1.6 We regularly remind employees of their data retention responsibilities.

3.1.7 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 Data Retention Policy and Schedule, any communications suspending data disposal and any specific instructions from the Data Protection Officer (DPO). 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 Responsibility of the DPO. The DPO is responsible for identifying the data that we must or should retain and determining 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 DPO handles the destruction of some records whose retention period has expired.

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 6.16.1 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:

5.2.1 Duplicates of originals that have not been annotated.

5.2.2 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.

5.2.3 Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of The Promise Scotland and retained primarily for reference purposes.

5.2.4 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 The Promise Scotland, 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.

6 RETENTION PERIODS

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 DPO.

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.

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 DPO.

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. The DPO 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.

7.3 The destruction of data must stop immediately upon notification from the DPO 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. Destruction may begin again once the DPO lifts the requirement for preservation.

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 Retention Policy: this Policy, together with the Data Retention Schedule 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.

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 UK GDPR as the principle of storage limitation.

ANNEX B - RECORD RETENTION SCHEDULE

The Promise Scotland Limited 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.

1. COMPANY AND CORPORATE RECORDS

TYPE OF DATA	RETENTION PERIOD	REASON
Accounting records.	3 years from the date they were made (private company)	Section 388(4) Companies Act 2006 (CA 2006)
Register of members.	Entries for former members can be removed 10 years after the date they ceased to be members.	Section 121, CA 2006
Register of directors.	Indefinite	Usual practice
Minutes of internal directors' meetings.	10 years from the date of the meeting	Section 248, CA 2006
Members resolutions passed other than at general meetings; minutes of general meetings, details of decisions provided by a sole director.	10 years from date of resolution, decision or meeting	Sections 355 and s358, CA 2006
Health and safety inspections, property management and asset records.	5 years	Health and Safety at Work Act 1974 and Prescription and Limitation (Scotland) Act 1973

2. HR AND BENEFITS RECORDS

TYPE OF EMPLOYMENT RECORD	RETENTION PERIOD
Recruitment records: • Completed online application forms or CVs. • Equal opportunities monitoring forms. • Assessment exercises or tests. • Notes from interviews and short-listing exercises. • Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.) • Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship.)	Six months after notifying candidates of the outcome of the recruitment exercise.
Immigration checks	Three years after the termination of employment.
Contracts: These may include: • Written particulars of employment. • Contracts of employment or other contracts. • Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends.
Payroll and wage records Details on overtime. Bonuses. Expenses. Benefits in kind.	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.

Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
Travel and subsistence.	While employment continues and for seven years after employment ends.
Personnel records: • Qualifications/references. • Consents for the processing of special categories of personal data. • Annual leave records. • Annual assessment reports. • Disciplinary procedures. • Grievance procedures.	While employment continues and for seven years after employment ends.

• Death benefit nomination and revocation forms • Resignation, termination and retirement.	
Records in connection with working time	
Working time opt-out	Three years from the date on which they were entered into.
Records to show compliance, including: • Time sheets for opted-out workers. • Health assessment records for night workers.	Three years after the relevant period.
Maternity records: • Maternity payments. • Dates of maternity leave. • Period without maternity payment. • Maternity certificates showing the expected week of confinement.	Four years after the end of the tax year in which the maternity pay period ends.
Accident records – these are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made.

3. PENSIONS RECORDS

TYPE OF DATA	RETENTION PERIOD	REASON
Name and address of scheme or provider of the automatic enrolment scheme used to comply with the employer's duties.	6 years	Employers' Duties (Registration and Compliance) Regulations 2010 (*SI 2010/5*) (Employers' Duties Regulations 2010) (regulations 5, 6 and 8).
Employer pension scheme reference.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).

Evidence scheme complies with auto-enrolment statutory quality tests.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).
Name, NI number, date of birth and automatic enrolment date of all jobholders auto-enrolled (and corresponding details for non-eligible jobholders and entitled workers who have opted in or joined).	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).
Evidence of jobholders' earnings and contributions.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).
Contributions payable by employer in respect of jobholders and dates on which employer contributions were paid to scheme.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).
If auto-enrolment postponement period used, records of workers who were given notice of postponement including full name, NI number and date postponement notice was given.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).
Auto-enrolment opt-in notices, joining notices and opt-out notices (original format).	6 years (4 years for opt-out notices)	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).
If employer is (or was) sponsoring employer of an occupational pension scheme, any document relating to monies received by or owing to the scheme, investments or assets held by the scheme, payments made by the scheme, contracts to purchase a lifetime annuity in respect of scheme member and documents relating to the administration of the scheme.	For the tax year to which they relate and the following 6 years	Registered Pension Schemes (Provision of Information) Regulations 2006 (*SI 2006/567*) (regulation 18).
Information relating to applications for ill health early retirement benefits, including medical reports.	While entitlement continues and for period of 15 years	Limitation period

	after benefits stop being paid.	
Death benefit nomination and revocation forms.	While entitlement continues and for period of 15 years after the death of member and their beneficiaries.	Limitation period

4. IT RECORDS

TYPE OF DATA	RETENTION PERIOD	REASON
General information about internally developed IT infrastructure, software and systems for internal use.	[5 years from decommissioning of system]	Business need
General information about externally developed IT infrastructure, software and systems for internal or external use.	[7 years from decommissioning of system]	Contractual obligation Limitation period
General information about internally developed IT infrastructure, software and systems for external use.	[7 years from decommissioning of system]	Contractual obligation Limitation period
Systems monitoring, (for example, to detect and prevent failures vulnerabilities and external threats).	[Current year plus 1 year] Consider whether records can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these logs for longer or indefinitely	Business need Contractual obligation Limitation period
Business continuity and information security plans.	[3 years from when the plan is superseded] Consider whether record can be fully anonymised after this period (or no personal data collected in first place) where there is a contractual or legal obligation to keep these plans for a longer period.	Business need Legal or contractual obligation

		Limitation period
Contracts and agreements (software licences, support agreements, hardware agreements etc.).	7 years from expiry of the agreement	Limitation period

5. SALES, MARKETING AND CUSTOMER RECORDS

TYPE OF DATA	RETENTION PERIOD	REASON
Marketing database records (e.g. lead generation, meeting feedback, contact data etc.).	2 years from last contact	Business need
Customer relations database records (e.g. call centre records, queries, meeting feedback, account history etc.).	5 years from last contact	Business need and limitation period.
Order fulfilment records.	5 years from completion	Limitation period and accounting requirement.
Opt-out/suppression lists.	Indefinite	Business and compliance need.
Evidence of consent to marketing (including electronic marketing).	While consent valid 5 years from date consent withdrawn or ceases to be valid	Business need Limitation period
Customer complaints handling	5 years from settlement or closure	Business need and limitation period

6. LEGAL RECORDS

TYPE OF DATA	RETENTION PERIOD	REASON
Legal advice and opinions (non-litigation).	5 years after life of the service or matter the advice relates to	Business need
Legal advice and other records relating to specific litigation or claim.	5 years from settlement or withdrawal of claim	Limitation period

Data subject rights requests	5 years from closure of request	Limitation period
Previous versions of policies, including IT policy, privacy policy, retention policy etc.	5 years form being superseded	Business need and limitation period in the event of a related claim
Monitoring and investigation requests	5 years from closure of investigation	Limitation period
Insurance claims	3 years after settlement	Limitation period