YORKSHIRE BUILDING SOCIETY

# YORKSHIRE BUILDING SOCIETY

# INFORMATION MANAGEMENT POLICY OVERVIEW

**Updated October 2023**

## Contents

# 1. Purpose

### The Purpose of the Policy

Information is critical to YBS – without it, our business would not operate.

We aim to provide real help with real lives, and making sure we manage our information properly and in line with legal and regulatory requirements are an important part of meeting this aim.

The purpose of this policy is to specify how information is to be managed across the Group in order to reduce the risk of:

- Information not being managed appropriately throughout its lifecycle, from planning to disposal
- Personal information of customers, colleagues and other data subjects not being handled in line with legal and regulatory requirements
- Information being incomplete or inaccurate, resulting in errors in regulatory and/or critical internal and external reporting, processes and operations

### Applicable Regulations and Legislation

There are various regulations and legislation that govern how we manage information. YBS must meet all applicable legal and regulatory requirements when managing information. These include, but are not limited to:

- Data protection regulations and regulator guidance, including but not limited to: (UK General Data Protection Regulation, EU General Data Protection Regulation (where relevant), , Data Protection Act 2018, the Privacy and Electronic Communications Regulations and the forthcoming E Privacy Directive)
- Financial services regulations
- Fraud and anti-money laundering regulations
- Information security standards (e.g. Payment Card Industry Data Security Standard)

### Requirements of the Policy

To adhere to the statements included within this policy and all other associated policies, standards and guidelines referenced throughout.

# 2. Scope

All YBS colleagues, including contractors and temporary workers. It applies to all locations in which they operate.

No one is excluded from the scope of this policy.

All information handled by YBS throughout its lifecycle, from collection to disposal. This includes:

- Both personal (e.g. information that relates to an individual – such as an employee or customer) and non-personal information (e.g. Management Information and information not relating to an individual)
- Information across any media and in any format (e.g. paper, electronic, removable media)

Structured and unstructured data (see section 3 for definitions).

# 3. Definitions

- **Data -** Data is raw, unorganised facts that need to be processed. Data can be something simple and seemingly random until it is organised and read in context. For example, each customer's loan amount is one piece of data.

- **Structured data** - Raw, unorganised facts or figures held and managed electronically, that feed business processes and form information. The Group's structured data is held in Core systems, databases, Data Warehouses and spreadsheets, etc.

- **Unstructured data** - Recorded information or an object which can be treated as a unit. This is wider than something in paper form, unstructured data could be a word processing document, a table, a report, microfiche, DIP'd document, documents in print systems and mailing rooms, posters, images, CCTV video, etc.

- **Information** - When data is processed, organised, structured or presented in a given context so as to make it useful, it is called information. For example, the average loan amount for all customers is information that can be derived from the given data, providing knowledge and insight.

- **Personal information** - Any information that, on its own or together with other information available, can be used to identify an individual. This includes information about customers, colleagues and other individuals, in whatever form it is held, for example. This includes Name, Address, DOB/POB, Contact number, Email address, NI Number, Bank Details, Card Details, CCTV, and Nationality. Plus other information that are personal information when identified to an individual, for example applications, property details, products, transactions, marketing permissions.

  *Note: The Data Protection Act defines personal information in relation to living individuals; however a duty of confidentiality towards a deceased individual's personal information remains.*

- **Sensitive/special category personal information** - Any personal information revealing racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data when used for the sole purpose of identifying an individual, physical or mental health, sexual life or orientation, commission or alleged commission of criminal offences and related proceedings and sentences.

- **Data subject** - Any living individual person who can be identified, directly or indirectly from the data available.

- **Information Lifecycle** - The journey that information takes during its lifecycle with YBS, from the point of collection to the point of destruction, in all formats and all storage media. The stages of the lifecycle are plan, obtain, store/share, maintain, apply/use, and dispose.

- **Incident** - An incident has occurred if information has been accidentally or unlawfully destroyed, lost, altered, disclosed without permission or accessed without permission. This includes incidents that are the result of both accidental and deliberate causes.

- **Breach of Data Protection** - Any one of the following instances may also constitute as a breach of data protection law:
  - Failing to meet our obligations as a data controller to maintain adequate records of processing
  - Failing to adhere to any of the data protection principles
  - Failure to meet any of the Data Subject Rights

- **Reportable Breach** - An incident, also known as a breach of security, likely to cause detriment to people's rights and freedoms has to be reported to the Information Commissioner Office within 72 hours.

## 4. Policy Statements

We want to provide real help with real lives. Critical to achieving this goal is maintaining the confidence of our colleagues, customers and regulators in the decisions we make to provide real help, based on accurate, complete, up to date and secure information.

We all have a responsibility in helping to achieve this aim and in embedding a strong culture of appropriate information management. Our obligations in this regard are described in the policy statements below.

### 4.1 Key Information Management Principles

All information - including personal information - which we handle must be appropriately managed throughout its lifecycle. To achieve this, we must adhere to the core information management principles at each stage of the lifecycle as defined below:

- **Plan** – you must define what information is needed, how it will be used and who will own it – obtaining approval by the relevant persons – prior to information being obtained. This includes carrying out assessments for all information (e.g. the Data Protection Impact Assessment (DPIA) and Data Management Checklist)

- **Obtain** – you must obtain information lawfully, fairly, transparently and for a specified purpose – only collecting the minimum information that is necessary to fulfil this purpose. Information must only be obtained once approval has been provided as part of the 'plan' stage

- **Store / Share** – you must store share and use information securely – protecting against unauthorised processing, loss, destruction or damage. You must only share information where strictly necessary, where you have been authorised to do so and once appropriate controls are in place

- **Maintain** – you must ensure information remains accurate and up to date, this includes maintaining inventories (e.g. the Record of Processing Activity (ROPA)) where required

- **Apply / Use** – you must ensure information is only used in the manner, and for the purposes, specified in the 'plan' stage and that individuals rights are provided for. You must seek relevant internal approvals, re-performing the 'plan' stage, where information is to be used for a new purpose

- **Dispose** – you must ensure information is only kept for as long as necessary (in line with the YBS, legal, and regulatory requirements) and subsequently archived and destroyed appropriately

### 4.2 Data Protection

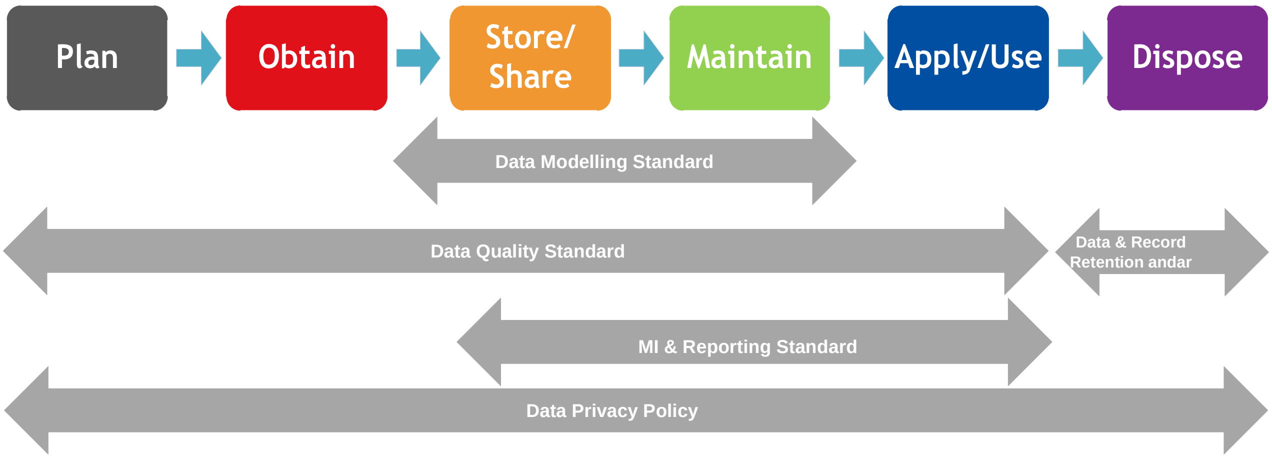
YBS is responsible for demonstrating accountability and compliance with relevant data protection laws. We must ensure that we manage our activities in respect of personal information both alone and with suppliers, in line with the UK GDPR seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Further explanation is available in the Data Privacy Policy.

### 4.3 Related Documents

Outlined below is our information lifecycle along with the applicability of standards in relation to each stage of the lifecycle.



## 5. Implementation and Monitoring

### Implementation

This Policy will be published on the YBS Intranet for access by all colleagues. Further publications of the policy where material updates have been made will be communicated to colleagues via a newsfeed and other relevant communication channels.

Various channels and methods will be used by the policy owner to raise awareness of the requirements of this policy, including the Data Stewardship training. Annual data protection training will be provided to all colleagues and contractors and that will cover the policy requirements relating to personal information.

### Monitoring

Compliance with this Policy will be monitored through first, second and third line monitoring, including:

- The Risk and Control Self-Assessment (RCSA) process;
- Annual self-assessments of key area, departments, systems and processes;
- Regular monitoring of information requirements by the first and second lines teams;
- Internal audits.

## 6. Approval

This Policy must be reviewed annually and updated where necessary. It must be recommended for approval by the Customer Services Divisional Risk Committee.

The Policy must be approved by Group Risk Committee.

# Appendix 1:  Description of roles and responsibilities

## Policy Owner

The Policy Owner is responsible for:

- Developing the policy document and ensuring that it remains up to date at all times.
- Reviewing the policy periodically and in the event of any significant change (e.g. legislative, regulatory, organisational, operational etc.).
- The Policy Owner should obtain endorsement for the policy from the Sponsor prior to seeking approval from the relevant Committee. Communicating the policy to all affected colleagues, ensuring that adequate supporting training is developed and delivered as required.
- Steps are taken to ensure compliance with the policy and report non-compliance to the Policy Sponsor and Enterprise Risk Management team;
- Ensuring the relevant policy guides are aligned to the policy.

## Policy Sponsor

The Policy sponsor is accountable for all aspects of the policy.

The Policy Sponsor is responsible for:

- Providing direction to the Policy owner as required.
- Supporting the Policy owner in discharging their responsibilities, specifically ensuring sufficient investment is made available to enable implementation and monitoring of policy adherence.
- Endorsing the Policy prior to it being submitted to the relevant governance committee for approval.

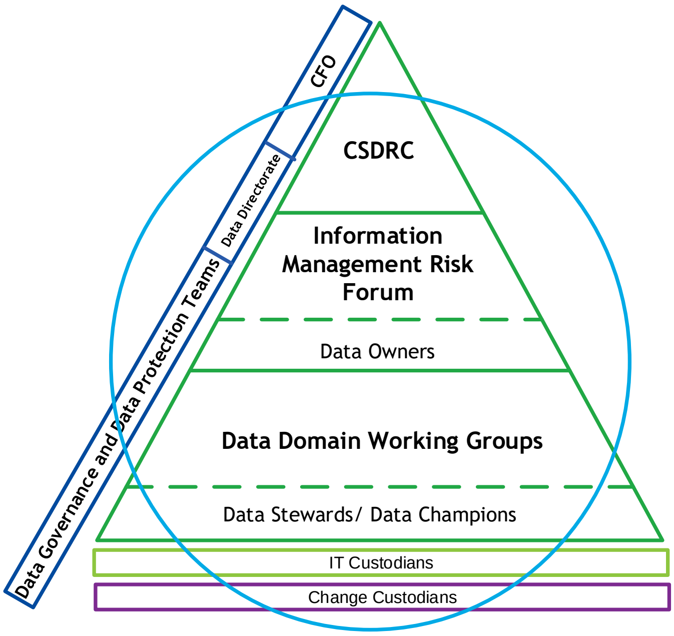
## Data Protection Officer

The Director of Compliance (and MLRO) has been appointed Data Protection Officer (DPO). The DPO’s role is to act independently and report directly to the Board on Data Protection matters, which is achieved through an annual DPO report. The DPO’s key responsibilities are to inform and advise YBS on its Data Protection obligations, and monitor compliance with Data Protection requirements.

## Appendix 2: Data Authority Structure

In order to formalise Data Management responsibilities, the YBS have established a Data Authority Structure. This provides the YBS with a structure of responsibility for the management of the Group's data, as outlined in the following diagram:

**YBS Data Authority Structure**


CFO
Data Directorate
Data Governance and Data Protection Teams
CSDRC
Information Management Risk Forum
Data Owners
Data Domain Working Groups
Data Stewards/ Data Champions
IT Custodians
Change Custodians

**Customer Service Division Risk Committee (CSDRC)**
Executive oversight of Risk Management and Change Management, including cascading regulatory change.

**Information Management Risk Forum**
(IMRF) Collaborative monitoring and oversight of the Societies Information Management Risk profile. Responsibilities for assessment of data risks and issues and effectiveness of controls, regulatory data requirement changes and escalation to CSDRC.

**Data Owners**
Senior colleagues accountable for core data categories within the organisation.

**Data Domain Working Groups**
Responsible for the oversight of day to day Data Management activities within the specific data domains, providing directive steer and appropriate escalation to Data Owners and IMRF where required.

**Data Stewards/ Data Champions**
Caretakers and supporting colleagues of data assets within their respective areas.

**Strategic & Operational IT Custodians**
Senior colleagues accountable for the IT Infrastructure design and IT Operational systems and procedures.

**Change Custodians**
Responsible for ensuring that data affected through the Change lifecycle is managed in line with Data Policies and Standards and appropriate for the needs of the business.

**All Colleagues**
Understanding and compliance with Data Management policies, principles and standards.

**Data Governance and Data Protection Teams**
Support, guide and facilitate Data Management practices and activities.

**Director of Data**
Director level oversight for Data and MI Governance & Control Framework

**Chief Finance Officer**
Executive Level Sponsor for Data Ownership and Data Quality and Data Protection.