YORKSHIRE BUILDING SOCIETY

INFORMATION MANAGEMENT POLICY OVERVIEW

Updated October 2024

Contents

YORKSHIRE BUILDING SOCIETY

1. Purpose

The Purpose of the Policy

Information is critical to YBS – without it, our business would not operate nor could we achieve our strategic ambitions. Information is the key to influence how we improve our customer experience, business resilience and decision making. The purpose of this policy is to support the Information Risk Management category and specify how information is to be managed across the Group to reduce the risk of:

1. Inappropriate management of information from planning / collection to the disposal of it.
2. Inappropriate management of personal information, (customers, colleagues and other data subjects) in line with legal and regulatory requirements
3. Inaccurate Information required for regulatory and/or critical internal and external reporting, processes and operations.
4. Poor quality information impacting automation / machine learning and inaccurate decision making.

Applicable Regulations and Legislation

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: (General Data Protection Regulation, Data Protection Act 2018, the Privacy and Electronic Communications Regulations and the 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) 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

This policy is agnostic of process and technology, including for example, AI and Machine Learning.

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, an email communication, a report, microfiche, scanned documents, documents in print systems and mailing rooms, posters, images including photographs, 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.

- **Data 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. These can include:
  - access to personal data by an unauthorised third party
  - deliberate or accidental alteration of personal data
  - sending personal data to an incorrect recipient (e.g. by post or email)
  - computing devices containing personal data being lost, stolen or unaccounted for
  - incorrectly disposing of IT equipment which may contain personal data
  - loss or availability of personal data by other means.

- **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.

In a world where data continues to grow at pace, with a reliance upon digital technology and expectations to access personalised services and products real-time, it is without doubt data is a core substance to any business. Data must also be protected, building trust with an ethical approach is important, to protect the privacy and rights of individuals, and ensuring regulatory expectations are met. Good Information management enables the business to deliver better outcomes, accelerating better access and use of data and insights, turning into more informed actions and decisions:

- Better commercial decisions to be more value creating
- Better understanding of our customers to enhance and personalise experience
- Better insights to drive increased reach and impact for 'Real help with Real life'
- Better flexibility and confidence to navigate through volatility, seeking opportunity and managing risk

All colleagues, suppliers and partners 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.

Figure 1:POSMAD data lifecycle

This responsibility is for all colleagues. To achieve this, we must all 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.
    - Identify the data that is critical to your business area and ensure this has clear ownership.
    - Always define what data you need, what question(s) you need it to answer or process you will use it for.
    - Agree business requirements with stakeholders before obtaining data.
    - Complete Data Protection Impact Assessment (DPIA).
    - Record data definitions and be consistent across the organisation, to establish a common vocabulary.
    - Understand the source of the data, it's transformation (calculations, exclusions, summaries etc.) and any impacts as it is processed.
    - Where the use, definition, source or location of data changes, you must revisit the risk assessment (DPIA).
    - Check the quality of the data in line with the definitions and support validation through automated verification or documented manual processes.

- **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.
    - Provision data – directly from source systems or via curated data stores such as the data warehouse, where possible.

- Automate the provision of data to reduce the risk of manual error.
- Co-ordinated or real time data access to address timing issues.
- Do not replicate data requests – can the same data source answer multiple questions?
- Check your obtained data is accurate and complete with validations/reconciliations before use.
- Report inaccuracies and associated risks, ensure these are managed with localised plans and in line with your risk controls (RCSA).

- **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.
  - Ensure Security and Access Controls. Implement robust security measures to protect our data. Protect data in transit and at rest.
  - Data should not be copy and pasted from other documents or shared via email, instead use trusted repositories and reference source data when presenting.
  - Collaborate across business functions to ensure one version of the truth.
  - Special considerations apply to personal data and furthermore detailed considerations to special category data, as outlined in our Privacy Policy.
  - Unauthorised loss or sharing inappropriately constitutes a data breach, which must be reported.
  - View Data as a shared asset. Treat data as a valuable resource to be shared across the organization.

- **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.
  - Regularly review and maintain data quality. Trusted, high quality data enables the Society to scale efficiently.
  - Eliminate data copies and movement, to minimise unnecessary data duplication.
  - Within process documentation, clearly document how data is used, processed and any transformations made.
  - Apply data quality rules to evidence trust in the data used. Report poor quality and raise associated risks and mitigate with localised plans utilising local Data Stewards.
  - Escalate and raise the risk of any inaccurate data found and manage through local action plans and risk control framework.

- **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 protected. You must seek relevant internal approvals, re-performing the 'plan' stage, where information is to be used for a new purpose.
  - Data Users should have appropriate skills and tools to apply/use the data.
  - Avoid key person dependencies and reduce end user computing to try and centralise data use.
  - Grow user knowledge through training and clearly documented processes.
  - Determine how your data can be used to drive insight, business change and prediction as well as reporting what has happened.
  - Report Data protection breaches where individual rights are not maintained, following the data incident process.

- **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.
  - Identify how long you need data and document this within the local data retention log. Manage disposal via automated routine where possible or scheduled manually with clear ownership.
  - Report from data source systems rather than copy data and store locally to reduce additional disposal requirements.

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.

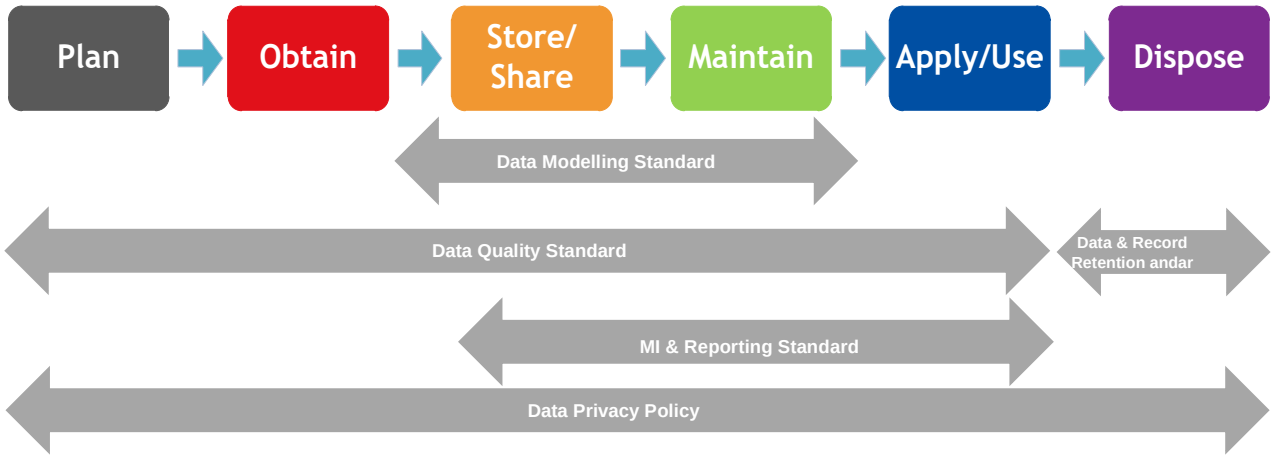

Figure 2: Related Documents

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 Operational Risk Committee (ORC).

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

A Data Protection Officer (DPO) is appointed within Compliance. 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, YBS have established a Data Authority Structure. This provides YBS with a structure of responsibility for the management of the Group's data, as outlined in the following diagram:

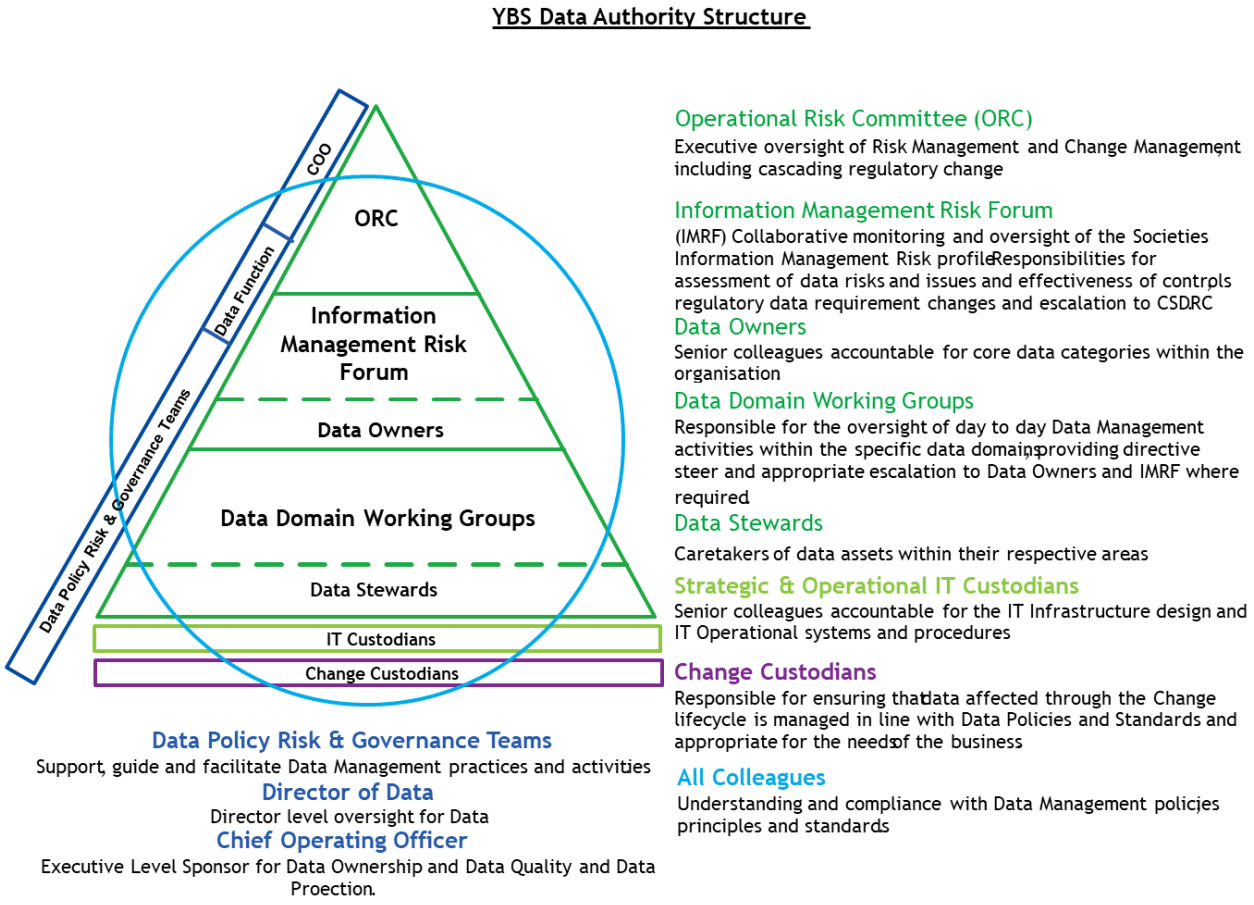

Figure 3: Data Authority Structure