Yorkshire Building Society

Information Management Policy Overview

Contents

1. Purpose

The Purpose of the Policy

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

We want to provide real help with real lives. Critical to achieving this goal is ensuring we maintain the confidence of our colleagues, customers and regulators in the decisions we make to provide real help, based on accurate, up to date and secure information. The purpose of this policy is to specify how information is to be managed across the Society 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

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: (General Data Protection Regulation, 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

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

This policy relates to 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 Society'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** - Information about an individual*, this includes details that identify them and also their financial dealings which includes their accounts and transactions.

  *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** - The individual to which personal information relates.

- **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 a number of individuals has to be reported to the Information Commissioner Office within 72 hours.

4. Policy Statements

We want to be the most trusted provider of financial services in the UK. Critical to achieving this goal and maintaining the trust of our colleagues, customers and regulators is appropriately managing the information we hold.

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 regards 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.
- **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 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 Data Protection Principles:

- To meet individuals rights;
- Reporting of Data Protection breaches;
- Evidencing compliance with Data Protection laws;

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 the Intranet and other relevant communication channels, including the Data Stewardship training. Annual data protection training will be provided to all colleagues and that will cover the policy requirements relating to personal information.

Monitoring

The Society operates a Three Lines of Defence (LoD) approach towards risk management. Each LoD has different responsibilities for managing the risk and therefore carries different actions.

The first LoD is directly responsible for the day to day management and control of risk throughout the business, generally within business functions. The second line is accountable for competent risk management across the society and overseeing the effectiveness and integrity of the Enterprise Risk Management Framework. The final LoD is providing independent assurance across the first and second LoD through our internal Audit function.

Compliance with this Policy will be monitored through the Three Lines of Defence, 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 by the Customer Services Divisional Risk Committee.