STANDARDS FOR SUPPLIERS

YORKSHIRE BUILDING SOCIETY	**WORKING WITH YBS**

1. INTRODUCTION

Yorkshire Building Society (YBS) exists to provide real help with real life. We do this by delivering our purpose ambitions of helping people have a place to call home and improve their financial wellbeing, underpinned by providing better value to our members. This is set out, along with our responsible business priority areas, within our ESG Strategy. You can find out more on our website (www.ybs.co.uk) and in our ESG Report.

Set out below are the minimum compliance standards which articulate YBS' expectations in relation to suppliers who provide products and services to YBS. They do not alter or eliminate any contractual requirements or other specifications set out in any contractual agreements entered between YBS and the supplier. YBS requires suppliers to comply with these standards (where applicable) and to also ensure that suppliers involved in their supply chain also comply with these standards. Some requirements may not apply to every supplier, depending upon the size, revenue, nature of the services or goods. We require our suppliers to understand and meet the requirements that apply to them.

We ask that the supplier review the standards in detail, and flag to us immediately any discrepancies between the supplier's company standards and YBS's expectations. YBS partner with Hellios to gather and assess suppliers' ability to meet these standards. Membership will be required to access Hellios (this is subject to a separate agreement between you and Hellios and may require fees to be paid).

Any discrepancies will be reviewed on a case-by-case basis and will not automatically mean YBS will not collaborate with the supplier, but that both parties build a plan to remedy any non-compliance and/or significant risk(s) over an agreed period.

These Standards for Suppliers were adopted on 7th Feburary 2025. YBS reserves the right to modify these Standards from time to time and suppliers will need to comply with those Standards as revised.

2. OUR COMMITMENT

As a mutual organisation, we were established over 160 years ago to deliver a positive social impact by helping working people to save, and by pooling these savings together, to buy a home of their own. Our commitment to doing the right thing for our customers, colleagues and our wider society continues today.

YBS commit to collaborating with our suppliers on a range of ESG topics such as community programmes and set high environmental standards to reach our ambition of Net-Zero by 2050. YBS have policies and procedures in place designed to help eradicate modern slavery, human trafficking, and operate within statutory standards to prevent injury and ill health in the workplace.

YBS always aims to treat suppliers with respect. YBS pays suppliers in accordance with the agreed payment terms and will seek to promptly resolve any disputes which may arise, in a fair and transparent manner.

YBS aims to achieve fair outcomes for all customers. Where customers have been identified as vulnerable, there is an enhanced duty of care to ensure good outcomes are received.

3. GENERAL - SUPPLIER STANDARDS

Supplier Community Impact

YBS encourages all suppliers and their employees to consider how they can get involved in local social and environmental community charity efforts by volunteering time and/or providing other types of support.

Supplier Employment Standards

- YBS expects suppliers to implement and maintain employment policies and procedures in compliance with UK law.
- YBS expects suppliers to have policies in place to prevent discrimination and harassment which are reviewed annually as a minimum.
- YBS expects suppliers to not tolerate any form of discrimination or harassment in their work force.
- Employees must be provided with adequate training and information, sufficient to enable them to fulfil their key responsibilities effectively. We expect employment background verification and screening checks are conducted before their employment starts in accordance with relevant laws, regulations, and ethics.
- Suppliers are expected to have processes in place to manage disciplinary and conduct issues and Disciplinary processes must be in place to manage any misconduct identified.
- Any employee concerns or complaints are dealt with in accordance with the supplier's stated policy / procedure.

Supplier Environmental Impact

- To ensure our supply chain emission reduction trajectory modelling is accurate and science based we seek the following information, annually, from our suppliers; Carbon footprint information (Scope 1 & 2 minimum) and a description on how the supplier is working towards a Net-Zero world. On Capital works projects (Property and IT only), we will seek a supplier to fill out a material usage and waste form.
- YBS expects its suppliers to be able to demonstrate what arrangements they have in place to protect the environment and how the products and services that they provide might support YBS in achieving its environmental aims.
- To aid with data collection, YBS utilises FSQS by Hellios to collate supplier emission data. YBS strongly encourages all its suppliers to sign up to FSQS by Hellios (third party) and report emission profiles through their verified questionnaire.

Ethical Business Practices & Modern Slavery

- YBS wants to work with organisations which share similar ethical principles. Checks have been implemented within procurement, which require suppliers to provide information on key factors such as regulatory compliance, adherence, and commitment to employment laws.
- Suppliers shall not engage in any activity, practice, or conduct that would constitute an offence involving Modern Slavery. Suppliers shall implement and keep a record of due diligence procedures for its own suppliers and subcontractors in its supply chains, to monitor and ensure that there is no Modern Slavery in its supply chains.

Fire, Health & Safety Standard

- Suppliers and contractors must comply with Health, Safety and Fire legislation which places legal duties on all businesses to protect all persons, including customers, from the risk of serious injury.

- All contractors work that falls under the CDM regulationsiwill be assessed for their suitability and competency by the YBS Supply Chain team, in conjunction with the Health & Safety team who will evaluate the contractors to determine the regulatory risk and the potential impact on service provisions. Once the approved contractors have satisfactorily demonstrated their ability to meet business's requirements (as well as legal requirements), they will be accepted onto the central supply register and will adhere to relevant procedures and applicable laws.

- The Health & Safety team will conduct audits on Property contractors which may vary depending on the nature of the work. Annual checks for property contractors are completed to confirm in date insurances and relevant Health and Safety certifications (where applicable).

Supplier Professional Standards

- YBS aims to maintain the highest standards of integrity in all business relationships and expects suppliers to do the same. Suppliers are expected to reject and report any business practice or approach which might be deemed improper and to declare to YBS any business or personal interests that affect or might be perceived by others to affect impartiality or decisions.

- Suppliers must have in place an adequate system of internal control, sufficient to ensure the quality and timeliness of the services provided to YBS and must support any assurance activity, including activities by regulatory and competent bodies, as per the contractual agreement.

- YBS expects suppliers to notify it, as soon as it is practical, of any events or incidents actually or potentially impacting on the service, customers, or reputation of YBS. Suppliers must have in place contingency plans to protect the interests of YBS and its customers in the event of any disruption to the services they provide.

4. VULNERABLE CUSTOMERS

YBS Group Vulnerable Customer Statement

Where customers have been identified as vulnerable there is a greater duty of consideration to ensure the delivery of good outcomes and third parties must ensure that their dealings are appropriate for their specific circumstances.

Vulnerable Customer Definition

A Vulnerable Customer is someone who due to their current personal circumstances may be susceptible to detriment and therefore may require us to engage with them in a different way to meet their individual needs.

Suppliers must ensure that they:

- Demonstrate they have the guidelines, codes of practice and sufficiently skilled colleagues to be able to identify potentially vulnerable customers and apply appropriate treatment.

- Consider the treatment appropriate to the nature of the individual vulnerable customer identified in line with YBS Vulnerable Customer Definition.

- Capture only information which is relevant and where appropriate agree suitable support solutions and a suitable support review period with the customer.

- Always attempt to gain explicit consent to record vulnerabilities. Where consent cannot be obtained this information should only be processed where not recording this would not be in the best interests of the customer.

- Review their approach annually to ensure it remains aligned with the YBS Vulnerable Customer Definition.

- Confirm to YBS, their continued adherence to the agreed approach on how third parties must deal

with YBS customers who are identified as vulnerable in line with the Financial Conduct Authority Handbook, particularly, Principle 6 of PRIN 2.1, which states that a firm must pay due regard to the interest of its customers and treat them fairly.

- Make use of available MI, Insight Data, and lead indicators to identify any emerging vulnerable customer risks.

5. FINANCIAL CRIME

YBS is committed to minimising the risk of financial crime, through the application of appropriate policies, procedures, systems, and controls to effectively deter, detect, prevent, and report any occurrence. YBS strives to ensure that high standards of financial crime prevention and awareness are maintained and expects suppliers with whom it has working relationships to do the same.

Suppliers must ensure that they:

- Comply with all applicable legal and regulatory requirements relating to financial crime including Money Laundering; Terrorist Financing; Financial Sanctions; Fraud (internal and external); Tax Evasion; Bribery and Corruption; Modern Slavery; and Human Trafficking.
- Have clear accountability and governance frameworks for the implementation of financial crime requirements within their business and the management of any control weaknesses identified. Relevant roles and responsibilities should be clearly defined.
- Have in place documented financial crime and linked policies and procedures (where appropriate to the services being provided).
- Complete the legal level of required Customer due diligence / ongoing Customer due diligence (including providing evidence to YBS upon request), where appropriate to the services being provided.
- Have appropriate controls in place to manage bribery and corruption risks, including provisions of the acceptance of gifts or corporate hospitality/entertainment, and have appropriate controls to identify, manage and record actual or potential conflict of interests.
- Have reasonable and proportionate controls in place to prevent the facilitation of tax evasion.
- Have reasonable and proportionate controls in place to detect and deter instances of Human Trafficking or Modern Slavery.
- Provide appropriate training for colleagues.

6. INFORMATION MANAGEMENT (DATA PROTECTION)

YBS has developed a robust approach to data and information management so that it can confidently meet YBS' regulatory obligations effectively and efficiently.

Suppliers must ensure that they:

- Comply with all data protection laws, regulations and principles for the services provided.
- Ensure that the processing of data undertaken on behalf of YBS is compliant with the requirements set out in the contract between the supplier and YBS.
- Implement controls and processes required to support YBS in the fulfilment of Data Subject Rights requests.
- Implement processes and controls to identify data breaches and report to YBS without undue delay in line with contractual obligations.
- Assist YBS to control and mitigate impact and detriment to customers and YBS following a data breach.

- Do not share data with third parties/sub-contractors unless agreed with YBS.
- Provide details of any appointed sub-processors who participate in the processing of the YBS data controls.
- Ensure the personal data it processes on behalf of YBS is adequate, relevant, and not excessive in relation to the purposes for which it is processed.
- Provide evidence of consent where necessary to demonstrate new data provided to the Group is done so compliantly.
- Ensure personal data is kept accurate and up to date.
- Take every reasonable step to ensure inaccurate personal data is securely deleted or amended without delay.
- Ensure any deletion of personal data which is no longer required is completed securely.
- Inform YBS of any of enforcements issued/ investigations undertaken by the ICO or any other Data Protection Authority.
- Do not transfer Personal Data outside the UK unless it has been agreed with YBS. Where YBS consent to any such transfer, this must also meet the relevant contractual requirements of YBS which include documenting any consent in writing and complying with any other terms and/or due diligence and risk assessments for international data transfers. Any verbal agreement or consent will not be sufficient. Any subsequent changes in any transfer destination or additional locations must follow the same process/contract terms and must be confirmed in writing.
- Ensure that upon termination of the relationship, YBS data is returned or securely disposed as per the contract.

7. COMPLAINT HANDLING

YBS has a zero tolerance for customer conduct failure and seeks to provide first touch resolution by resolving customer complaints at the first point of contact and in a clear, fair, and consistent manner.

Suppliers must ensure that they:

- Signpost the Complaint Policy and ensure it is accessible for all their colleagues.
- Make themselves aware of customers with vulnerable circumstances. Most customers can make informed decisions regarding their financial affairs; however, you need to be aware that you may discover customers with vulnerable circumstances in the process of managing their complaint. Where vulnerability is identified consideration must be given to the impact of the complaint on the customers' vulnerability, making sure to prioritise the complaint accordingly. Please refer to the Vulnerable Customer statement (Section 4 of this document).
- Allow customers to contact them through any of the supplier's available communication channels and by any reasonable means to make a complaint without any barriers.
- Consider if a customer should receive redress to put them back in the position, they would have been had the error not occurred and compensate them for the distress and inconvenience experienced.
- Treat each customer as an individual assessing the financial and non-financial impact of the complaint on them.
- Maintain a Complaint Policy that identifies complaints as individual issues raised by individual complainants. However, periodically, a single complaint may identify a wider or systemic issue. In

such an event YBS must be notified via their Supplier Manager.

- Identify complaints promptly and investigate thoroughly, honestly, and openly with the complainant(s) being kept informed of the progress and outcome of the investigation using clear communication and plain English. Complaint handling must be flexible and responsive to the needs of each individual and will obtain a quick and effective resolution of their complaint.

- Prevent discrimination against customers who have complained either through the handling process or in subsequent interactions.

- Undertake root cause analysis of complaints generated because of their servicing of the YBS customer and provide insight to YBS regarding this and any resulting actions.

- Comply with the regulations of the Financial Conduct Authority (FCA) as set out in the FCA's Dispute Resolution (DISP) Sourcebook.

- Have a process in place to ensure where a complaint relates to actual or potential data breaches these are reported as appropriate to the Information Commissioner's Office (ICO).

8. BUSINESS CONTINUITY

YBS' approach to managing business continuity is to protect the Society's Important Business Services by ensuring such services are available for YBS' customers when they need to use them.

Suppliers must ensure that they:

- Establish a Business Continuity / Disaster Recovery Policy, which is approved in accordance with the supplier's governance structure, which provides a framework for setting Resilience & Continuity objectives and defines the standards for their implementation and operation. This policy must be reviewed and updated at defined intervals, on a 12-monthly basis as a minimum.

- Have a defined Incident, Crisis Management Framework (including incident communications) to ensure that incidents and crises will be identified, managed, and communicated to YBS in line with agreed service levels and agreed Recovery Time and Point Objectives (RTO / RPO).

Additional requirements are mandated if YBS deem the supplier to be critical. All critical suppliers will be advised if this is the case:

- Provide sign-off on an annual basis to the respective YBS Supplier Relationship Manager that the services outlined in the contractual arrangement can be met and understand the role they play in the Recovery Time Objective of the Important Business Services.

- Define and document the roles and responsibilities of all key person dependencies that underpin the services supporting the YBS Important Business Services.

- Ensure that key colleagues supporting YBS Important Business Services are aware of their roles & responsibilities in relation to the services supporting YBS Important Business Services on a minimum twelve-monthly basis through inductions or training.

- Identify fourth party suppliers that are critical to the delivery of services supporting YBS Important Business Services and should evidence their ability to meet Important Business Service Impact Tolerances.

- Identify and document those applications/systems that are critical to the delivery of services supporting YBS Important Business Services.

9. INFORMATION SECURITY

YBS' appetite is to be secure and resilient to cyber threats. It expects both itself and suppliers to be able to recover after an event and be confident and effective in a digital world.

Suppliers must ensure that they:

- Comply with all relevant legal and regulatory obligations, including data protection laws, and contractual requirements for the services provided.

- Maintain the necessary technical and organisational information security measures to prevent any unauthorised use, alteration, or destruction of YBS information assets by any employee or approved subcontractor.

- Record details of all systems which store, process or transmit the YBS' information assets, and be able to provide data flow diagrams to describe these activities on demand.

- Maintain documented technical and organisational information security controls and audit the performance of these controls on a regular basis.

- Maintain an information security policy, approved by senior management, and regularly reviewed, which must contain as a minimum:
    - Require only the use of approved devices when handling YBS information assets.
    - Cover the acceptable use of approved devices for handling YBS information assets.
    - Prohibit the use of other devices for handling YBS information assets.
    - Explicitly state workers' obligations and requirements for handling YBS information assets in terms of the protection of confidentiality, integrity, and availability.
    - Prohibit the unauthorised disclosure or handling of YBS information assets.
    - Define an information classification scheme that must be applied to all data and must describe the requirements for handling data of each classification type.

- Not outsource the handling or processing of YBS information assets without the prior written consent of YBS.

- Ensure that its personnel (see Section 11 (Supplier Personnel) for definition) are subject to adequate background checks and vetting prior to employment or engagement.

- Ensure that information security awareness and training programmes are provided for all employees upon hire and on at least an annual basis.

- Protect all YBS Information by adopting a 'clear desk' policy and disposing of YBS Information assets in a secure manner when no longer required.

- Must ensure that their premises and facilities are secured with effective physical security controls including the use of auditable access system with access tokens, intruder detection system and alarm, 24/7/365 onsite security monitoring via CCTV or onsite Security Officers.

- Protect any YBS information assets or systems provided to YBS from external attack by using a set of security technologies (e.g., firewalls, intrusion prevention systems, anti-virus software scanning inbound data etc.) and techniques (e.g., network segregation, the use of a Security Operations Centre (SOC) etc.).

- Enforce the use of secure access methods which as a minimum should include unique user accounts, effective access management processes, strong complex passwords or two-factor authentication, regular password changes. In addition, any remote access to their systems shall be via secure, encrypted remote access methodologies utilising two-factor authentication.

- Encrypt confidential YBS information assets in transit and at rest using strong cryptography in accordance with industry good practice and in accordance with YBS' requirements as notified to the supplier from time to time.

- Deploy anti-malware technologies at all ingress/egress points and on all equipment used to store, process, or transmit YBS information assets and ensure that it is configured to update regularly and cannot be tampered with.

- Follow secure development practices in accordance with industry good practice, ensuring that all developers are skilled and trained in secure development practices and integrating appropriate security practices and testing into the software development lifecycle.

- Not use Personally Identifiable Information provided by YBS in any testing or development activities without prior consent.

- Regularly test IT systems through penetration testing and/or vulnerability scanning, as appropriate, and shall ensure that any security vulnerabilities are assessed and remediated in line with their risk profile. Where critical vulnerabilities are found in systems hosting YBS data, YBS must be informed as soon as possible.

- Maintain measures to identify, detect and respond to any Security incident or breach relating to the supplier's systems in a timely manner.

- Ensure that the YBS is made aware of any incidents which may impact on the confidentiality, integrity, or availability of YBS information assets as soon as is practical.

- All subcontractors, suppliers or third parties involved in the provision of services to the YBS must maintain an appropriate level of security and must be regularly assessed.

- Do not use or purchase cloud-based services to store or process YBS information assets, without the express written authorisation of YBS.

- YBS Information Security team maintains the right to audit any supplier on a periodic basis or following any incident which affects YBS information assets, this audit may include self-assessment questionnaires, validation of certifications, on-site visits or other controls testing dependent on the nature of the service and the risks to YBS information assets.

10. INFORMATION TECHNOLOGY

YBS has core operating principles in place to ensure operational resilience through providing reliable, stable, secure, and responsive systems for its customers, colleagues and other stakeholders.

Suppliers must ensure that they:

- Comply with contractual agreements and schedules of work for all elements of technology supporting YBS services.

- Comply with all applicable legal and regulatory requirements for the services provided.

- Demonstrate that applications and systems are designed, developed, tested and implemented in accordance with YBS requirements.

- Document knowledge and information to support processes, skills transfer, and training, as required and made available on request including technical documentation and user manuals.

- Operate a Standard for managing the implementation of all types of technology change and provide adequate notice to YBS of such changes.

- Provide adequate methods for integration with other YBS systems, when required and in line with contractual SLAs.

- Maintain appropriate IT service management application to manage all IT changes.

- Maintain implementation and back-out plans and ensure these are tested before promotion to live/production for all services (new implementations or significant changes).

- Monitor and maintain IT services to ensure resilience, minimising potential disruption to YBS services in line with contractual SLAs.

- Design critical services for high availability and disaster recovery, in accordance with YBS definitions and standards.

- Maintain IT hardware and software at version levels that allow YBS and the supplier (as per contractual obligations) to support, maintain, secure and/or patch where required.

- Implement processes to manage and communicate incidents and problems to ensure resilience minimising potential disruption to YBS services in line with agreed SLAs.

- Maintain an accurate record of technology assets.

- Create and maintain an inventory of configuration information, aligning with the relevant change and configuration management processes associated with providing contracted services to YBS.

- Maintain IT systems and assets in accordance with the supplier's recommended service intervals and specifications or other requirements as agreed.

- Maintenance windows and schedules are agreed with YBS to minimise potential disruption to YBS services in line with agreed SLAs.

11. SUPPLIER PERSONNEL

YBS' appetite is to minimise risks arising from the engagement and use of supplier personnel (being any employees, workers, temporary staff, agents, consultants, sub-contractors, directors or other personnel of the supplier or any member of the supplier's group involved in the provision of products or services to YBS). It requires certain assurances and expects certain minimum standards to be met by suppliers and supplier personnel.

Suppliers must ensure that they:

- Only provide YBS with supplier personnel who fall within the categories listed below or otherwise not subject to the off payroll working legislation (including, but not limited to, the Income Tax (Earnings and Pensions) Act 2003 (as applicable)):
    - Employees employed directly under a contract of employment with the supplier subject to UK PAYE and NICs on payments relating to their work with YBS.
    - Workers employed or engaged under an agreement with the supplier or via an agency or umbrella company subject to UK PAYE and NICs on payments relating to their work with YBS.
    - Offshore workers who are not subject to UK PAYE and NICs and will become subject to UK PAYE and NICs because of the services being performed.

- Do not provide supplier personnel who operate through personal services companies or other worker intermediary companies, at any level in the supply chain, without YBS' prior written approval. Such arrangements will be on an exceptional basis and must be identified to YBS prior to any supplier onboarding or contracting being completed.

- Any supplier personnel not falling into a group above will require YBS sign-off prior to entry into contract arrangements or commencement of any services to YBS.

- Co-operate with YBS and provide such reasonable assistance or information as YBS may request from time to time relating to the employment status of supplier personnel.

- Are responsible (and where applicable, shall procure any third parties such as agencies or umbrella companies shall be responsible) for all matters in relation to the supplier personnel including, but not limited to, (i) procuring and complying with any requirements for any work permits, visas, rights of residence or other similar requirements; and (ii) the payment of all salary and remuneration, National Insurance contributions, income tax or other charges and deductions required by law including

submitting all necessary returns required under applicable law and maintaining suitable and proper records in respect of all supplier personnel.

- Provide supplier personnel who are suitable and possess the necessary qualifications, experience, knowledge, and skills for their role always to provide the services to YBS with all reasonable skill, care, and diligence.

- Conduct appropriate vetting checks on supplier personnel to ensure that (i) they have the relevant skills, experience and suitability to be involved in the provision of services to YBS; and (ii) no supplier personnel are engaged or employed in relation to the services to YBS whose previous background would reflect adversely upon YBS (including any individuals convicted of serious criminal offences).

12. CONSUMER DUTY

YBS abides by the Consumer Duty finalised guidance published by the Financial Conduct Authority (FCA), with effect from 31st July 2023.

Suppliers must ensure that they:

- Comply with the requirements set out by the FCA in the Consumer Duty finalised Guidance that are relevant to all activities conducted by the firm.

- Consistently deliver good outcomes for retail customers

- Monitor and regularly review the outcomes that customers are experiencing in practice and take action to address any risks to good customer outcomes.

- Provide any Management Information required by YBS to evidence the delivery of good outcomes within reasonable timescales.

- Consider the needs, characteristics, and objectives of customers – including those with characteristics of vulnerability – and how they behave, at every stage of the customer journey.

- Communicate and engage with customers so that they can make effective, timely and properly informed decisions about financial products and services and can take responsibility for their actions and decisions.

- Not seek to exploit customers' behavioural biases, lack of knowledge or characteristics of vulnerability

- Support customers in realising the benefits of the products and services they buy and acting in their interests without unreasonable barriers