Information Security.

Information Security is necessary to protect our customers, our colleagues, and our business. Our Information Security Policy involves a series of internal policies, procedures and systems designed to protection our information assets, proportionate to the scale and nature of our current business.

Assessing and managing Information Security risk is a vital component to achieve the correct customer, commercial and regulatory outcomes. The Information Security Policy defines the key risk principles followed to support operational adherence to the Enterprise Risk Management Framework and associated regulations and legal requirements. The Information Security Policy is applicable to all confidential information within Together, from company information like our policies, management documents and plans, to the personal and financial information of our colleagues and customers.

Our Vision and Beliefs.

The Group's Vision is to be the most valued lending company in the UK, which drives the design ethos for building both the products and the operational processes that support them.

Our beliefs form the foundation of the Group policy design criteria. This criteria has informed the risk policies with a line of sight from the defined risk and its ownership, the risk appetite, where it arises, and the manner of its control.

Accountability.

Our Information Security Policy, along with all our other Policies and Standards, apply to all colleagues including temporary colleagues, contractors, suppliers and third parties that carry out activities on behalf of the Group and its subsidiaries.

Our Chief Compliance Officer sponsors adherence to the Information Security Policy at Board Risk Committee. Our Head of Data Protection and Information Security is responsible for developing the Information Security Policy, securing the review and approval of the policy from the appropriate stakeholders, overseeing and reporting on the Group's compliance with its requirements, and providing assurance on the implementation of key controls.

Continued overleaf...

The Head of Data Protection and Information, together with the wider Group Risk department and Group Technology Services, maintains the Information Security Policy, other supporting Information Security related policies and procedures, and provides appropriate guidance materials to support effective implementation.

The Group executes its system of internal controls and risk management activities through the three lines of defence model, at both a Group and divisional level.

Purpose.

Our Information Security Policy is intended to provide a framework which creates a robust and secure environment. The Group is committed to the highest standards of information security and confidentiality.

The purpose of the Information Security Policy is to ensure that Information Security risks are managed in line with the Group's strategic plan, regulatory and legal requirements, and within the Board approved risk appetite. It outlines the approach we have in place to minimise the risk of unauthorised or inappropriate use of information assets which may impact on the integrity, confidentiality or availability of information.

Underpinning the policy is a range of frameworks and controls which include (but is not limited to):

- Annual training for all colleagues, contractors, agency staff and those on fixed-term contracts
- Appropriate technical and organisational security measures
- Reporting and oversight through our three lines of defence model of risk management
- Assurance from our independent audit function

The Information Security Policy is also subject to at least an annual review in order to ensure it remains accurate and fit for purpose.