



Administration

Owner	Compliance, Liontrust Asset Management Plc
Governance Owner	Financial Crime Prevention Committee
Effective Date	January 2023
Review Cycle	Annually
Document Distribution	External

Scope

This statement is designed to provide comfort to external parties on Liontrust’s internal policies and procedures. The following will be covered:

- Anti-Bribery & Corruption
- Anti-Money Laundering
- Whistleblowing

The use of “Staff” in this document refers to both Partners and Employees.

Code of Conduct

Liontrust expects all employees to conduct themselves responsibly, with integrity, and with investor’s best interests at the core of what they do. All Liontrust employees must comply with our internal policies and procedures, as well as the Financial Conduct Authority’s (FCA) Conduct Rules under the Senior Managers and Certification Regime (SM&CR) – these principles are reinforced through the performance management and training and development processes. We have also adopted the Chartered Financial Analyst Institute’s Asset Manager Code, a voluntary code of conduct to help asset managers practice ethical principles that put client interests first.

Compliance

Liontrust operates across both the United Kingdom and the European Union and as such, is subject to authorisation and ongoing compliance with regulatory requirements from multiple regulatory bodies. These include the Financial Conduct Authority (FCA) in the UK, the Central Bank of Ireland (CBI) in Ireland and the Commission de Surveillance du Secteur Financier (CSSF) in Luxemburg.

Liontrust’s Chief Compliance Officer, who holds the SM&CR responsibility for Compliance Oversight and Financial Crime Compliance (SMF16 / SMF17) in the UK, is supported by a nine-strong team of Compliance professionals who support the Chief Compliance Officer in implementation of policies, procedures and controls, as well as ongoing monitoring activity, cyclical and thematic reviews, regulatory change management and training delivery.

Financial Crime Compliance

Liontrust takes its obligations to tackle financial crime seriously; not only does it pose a reputational and legal risk to the firm and its stakeholders, it is also the right thing to do. Liontrust will not knowingly allow itself to be used in connection with money laundering or financial crime. We assess and manage the risks associated with Money Laundering and Financial Crime in a variety of ways and these include considering the procedures adopted to identify customers on a regular basis in association with our Third-Party Providers, obtaining regular updates on any

unidentified customers and considering the action taken to resolve those outstanding. We undertake annual, or more frequently as the risks increase, monitoring reviews of identification procedures and sample paperwork relating to transactions.

We keep abreast of industry developments and seek to ensure that any significant developments are noted in Staff training and implemented in our processes and policies where appropriate. We will proactively manage any problem accounts, where the identity is difficult to confirm and make the necessary regulatory reports as appropriate. Liontrust or its staff are not permitted to offer, make or receive improper payments such as bribes or kickbacks (whether to government officials or to private sector customers), or excessively generous business courtesies. In addition Liontrust, or its Staff should never use a third party to undertake any act or function on their behalf, which would circumvent these policies. We are committed to ensure that our Staff are provided with sufficient training in relation to their respective roles in relation to the prevention of financial crime and money laundering.

Anti-bribery and Corruption

Liontrust is committed to demonstrate the highest level of integrity in conducting its business and, as such, has established a number of controls to support the prevention of bribery and corruption. All employees receive mandatory annual training on anti-bribery and corruption, as well as at the point of on-boarding, and are asked to make at least annual attestations on any potential conflicts which may give rise to risk of bribery or corruption occurring. Due diligence processes are in place for any contracted parties or outsourced providers, and these are reviewed in line with the internal Liontrust Counterparty Selection and Management Policy. Liontrust also has guidelines on receiving and giving inducements, staff must act honestly, fairly and professionally in accordance with the best interests of its clients. Any gift or hospitality given or received (in line with the relevant policy) should not impact the business judgement of Liontrust or its stakeholders and is handled in a transparent and fair manner. All employees are bound by the policy on anti-bribery and corruption and annually attest on understanding of their obligations under the policy.

Whistle Blowing

Liontrust actively seeks to foster a culture of openness, transparency and fairness. As part of this, it is essential to have a mechanism in place to allow employees to raise concerns without fear of reprisal, victimisation or harassment. All employees are made aware of and have access to our anonymous Whistleblowing reporting forms through which they can submit concerns on malpractice or wrongdoing within Liontrust to Compliance. All employees are also made aware of their ability to make a Whistleblowing report directly to the FCA.

Data Protection

Liontrust is committed to protecting the personal data of its staff, customers and contacts and using it in the appropriate manner. We recognise the rights afforded to individuals by data protection legislation and must advise stakeholders of the fact that we process their personal data and the specific purpose for which we do so.

Our Data Protection Policy reflects the legal requirements set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 by ensuring Liontrust:

1. is clear about how personal data must be processed and the expectations for all those who process personal data on its behalf;
2. complies with the relevant data protection law(s) and regulation, and with industry good practice;
3. protects the firm's reputation by ensuring all personal data is processed in accordance with data subjects' rights; and
4. protects itself from the risks of personal data breaches and other breaches of data protection law.