Finance Division

FINANCIAL COMPLIANCE POLICY

1. OVERVIEW AND PURPOSE

1.1 The University is committed to the highest standards of professional ethical conduct and integrity, especially in matters relating to management of its finances. This also includes ensuring adherence to all relevant legislation[1].

1.2 This policy describes offences in the areas of bribery, fraud, tax evasion, money laundering, and sanctions compliance; it also makes clear responsibilities of the University community in relation to these matters and outlines the University's approach to ensuring that it is not committing any such offences.

1.3 This policy will also signpost to various related supporting documents (e.g. procedures), which must be considered alongside this policy and adhered to, to ensure compliance with this policy.

2. SCOPE

2.1 This policy applies to, and must be adhered to, by all staff. For the purposes of this policy, 'all staff' includes the following, whether remunerated or not:

- Senior managers, officers, and directors;
- Employees (whether permanent, fixed-term, temporary, or casual);
- Contract, seconded, and agency staff;
- Volunteers, apprentices, and interns; and
- Others associated with (i.e. performing services for or on behalf of) the University (for example, agents, consultants and other suppliers).

2.2 This policy applies to all activities carried out by the University and any subsidiaries, majority controlled associated undertakings, and joint ventures of the University unless the subsidiary, associated undertaking or joint venture has an equivalent policy.

3. RESPONSIBILITIES

3.1 Council

3.1.1 Council is responsible for ensuring the establishment and monitoring of systems and financial and operational controls, to enable the University's compliance with all relevant statutory and regulatory obligations governing financial management as set out in this Policy.

[1] Including the Bribery Act 2010; the Criminal Finances Act 2017; the Proceeds of Crime Act 2002, Money Laundering Regulations 2017, the Terrorism Act 2000, the Sanctions and Anti-Money Laundering Act 2018, the Fraud Act 2006 and the Economic Crime and Corporate Transparency Act 2023.

3.2 **Vice-Chancellor**

3.2.1 The Vice-Chancellor shall foster an open culture in which fraud and other non-compliance is never acceptable.

3.3 **Chief Financial Officer (CFO)**

3.3.1 The Chief Financial Officer is responsible for developing, implementing and maintaining adequate systems of financial management and internal control, including the provision of appropriate training, to mitigate/minimize the risk of non-compliance with relevant statutory and regulatory obligations governing financial management as set out in this Policy.

3.4 **Executive Deans and Professional Services Directors**

3.4.1 Executive Deans and Professional Services Directors are responsible for the implementation of this policy within their Faculty/Division, including by taking all reasonable steps to ensure that staff in their Faculty/Division are aware of and are compliant with this policy.

3.5 **All Staff**

3.5.1 All staff are responsible for ensuring that they comply with this policy, including maintaining and monitoring compliance with internal controls and agreed policies and procedures; immediately reporting details of any suspected breaches, whether by an employee or an external organisation, and assisting in the investigation of suspected breaches.

4. **POLICY**

4.1 **Anti-Bribery**

4.1.1 A bribe (as defined by the Bribery Act 2010) can be any form of financial or other advantage which is intended to act as an inducement or reward in order for someone else to misuse their position or improperly perform their function. A bribe is typically designed to achieve a commercial, contractual, regulatory, or personal advantage for the bribe payer, or be used to try to gain some reputational benefit for the bribe payer or another person.

4.1.2 The Bribery Act 2010 creates a number of bribery offences that an organisation such as the University, as well as individuals, can be liable for. These offences are:

- Bribing another person;
- Being bribed;
- Bribery of a foreign public official; and
- Failing to prevent bribery, when a bribe is paid on an organisation's behalf in order to win or retain business or a business advantage.[2]

[2] It is important to note that this offence applies to bribes paid in both the UK and overseas, and that the organisation does not need to have known about it.

4.1.3 In addition, if an individual with management responsibility turns a blind eye, consents to, or connives in bribery, they can be separately prosecuted.

4.1.4 The sanctions for bribery offences are severe; they include up to ten years' imprisonment for individuals and unlimited fines for organisations, as well as significant reputational damage.

4.1.5 Adherence to the policy should prevent a bribery offence from being committed. Related supporting processes and guidance issued alongside this policy also provide detail on red flags and practical application of these rules:

- Do not make payments to someone (or favour them in any other way) if you know that this will involve the misuse of their position;
- Do not misuse your own position in connection with payments (or other favours) for yourself or others; and
- Do not deliberately use advantages to try to influence foreign public officials for business reasons; if you need to promote the University's business with a foreign public official, agree in advance how to approach this with your line manager.

4.1.6 Facilitation payments - typically small unofficial payments to speed up an administrative process or secure a routine government action by an official (most frequently encountered in overseas jurisdictions with perceived high corruption risks) – are also bribes and thus prohibited by this policy.

4.1.7 This policy does not prohibit reasonable and proportionate gifts and hospitality being given to or received from third parties. However, relevant procedures should be followed including recording gifts and hospitality as required via the University's Gifts and Hospitality Register.

4.1.8 Donations received by the University must adhere to this policy and the University's Donations Policy.

4.1.9 The University does not make contributions to political parties. It is only open to the University to make charitable donations at an institutional level in limited prescribed circumstances, and any such requests should first be referred to the Chief Financial Officer for approval.

4.2 Anti-Money Laundering

4.2.1 The statutory and regulatory framework surrounding money laundering is centred on the following:

- Proceeds of Crime Act 2002 ('POCA')
- Money Laundering Regulations 2017
- Terrorism Act 2000

4.2.2 Though the Money Laundering Regulations apply only to specified sectors which are at higher risk of being used for money laundering or terrorist financing, which do not include universities/Higher Education institutions, they establish best practice standards some of which the University adopts. For example:

- Implementing procedures to enable the identification and reporting of suspicious activity;
- Having procedures in place for customer identification in relevant circumstances; and
- Maintaining adequate records of transactions.

4.2.3 Money laundering can be defined as the process by which the proceeds of a crime are dealt with in a way that disguises their origins, and the primary offences are contained in sections 327 to 329 of the Proceeds of Crime Act 2002.

4.2.4 The legislation outlines a number of money laundering offences:

- Concealing, disguising, converting, and transferring criminal property or removing it from the UK;
- Entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use, or control of criminal property by or on behalf of another person; and
- Acquiring, using, or possessing criminal property.

4.2.5 A full list of associated offences can be found in related supporting documents and include due diligence and disclosure offences, along with the specific rules and checks that apply to the different types of transactions as outlined below:

- Transactions that lack a clear academic or business rationale;
- Requests for refunds to different accounts than the original payer;
- Overpayments followed by refund requests;
- Unusual urgency or pressure to process payments or refunds.

4.3 **Tax Evasion**

4.3.1 Tax evasion refers to cheating the public revenue or fraudulently evading UK tax.

4.3.2 Foreign tax evasion means evading tax in a foreign country, provided that the conduct is an offence in that country and would be a criminal offence if committed in the UK.

4.3.3 Tax evasion facilitation means being knowingly concerned in, or taking steps with a view to, the fraudulent evasion of tax (whether UK or foreign) by another person, or aiding, abetting, counselling, or procuring the commission of the offence.

4.3.4 Where any of the above involve deliberate action, or omission with dishonest intent, there is an element of fraud, and these constitute criminal offences. Under the Criminal Finances Act 2017, a separate criminal offence is automatically committed by an organisation such as the University where tax evasion is deliberately and/or dishonestly facilitated by a person acting in the capacity of an ‘associated person’ to that organisation (which includes the University’s employees or those performing a service on the University’s behalf, which can also include venture partners and subsidiaries).

4.3.5 Supporting documents should be consulted for a list of ‘red flags’, i.e. situations that raise concerns around tax evasion.

4.4 **Sanctions**

4.4.1 This part of the policy applies to any activity with individuals or entities from, or with links to, sanctioned countries. A list of sanctioned countries is available on the University’s Sanctions webpages. For the purposes of this policy, sanctioned countries are divided into two categories as determined by the University’s banking partners:

a) **Narrowly Restricted Countries (NRCs)**: These countries are subject to closely cast sanctions , the majority of which are focused on the prohibition of activities relating to the trading of weapons.
b) **Broadly Restricted Countries (BRCs)**: These countries are subject to a wide range of sanctions measures with a significant list of individuals and entities subject to sanctions.

Examples of University activities which may be impacted by sanctions include donations, student payments, provision of consultancy services, recruitment partnerships and other strategic partnerships, procurement of goods and services (including engaging new suppliers), research grants and research agreements. Note that this is not an exhaustive list, and sanctions could apply to potentially any University activity.

4.4.2 Sanctions checks

4.4.2.1 Staff members of the University shall not enter any arrangement or transaction which is prohibited by sanctions. Staff members shall therefore carry out sanctions checks and risk assessments as set out in this policy.

4.4.2.2 Guidance on how to conduct sanctions assessments is available in the Sanctions Assessment Procedure document.

4.4.2.3 Where dealings with an individual or entity from, or linked to, a narrowly or broadly sanctioned country are ongoing, entities should be routinely re-checked. Guidance on this process is available in the Sanctions Assessment Procedure document.

4.4.2.4 Where required, the University will also comply with the procedures required by its banking partners in relation to sanctions.

4.4.3 Risk assessments and approvals

4.4.3.1 The route of risk assessment and approval differs depending on whether the assessment involves an individual or entity based in, or with links to, a Narrowly Restricted Country (NRC) or a Broadly Restricted Country (BRC).

4.4.3.2 Narrowly Restricted Countries (NRCs)

a) For any proposed transaction or arrangement between a staff member or the University and an individual or entity based in, or with links to, a Narrowly Restricted Country (NRC), a nominated member of the responsible Professional Services (PS) Division should complete a sanctions check in accordance with the Sanctions Assessment Procedure document.

b) If it is identified that there **are** sanctions which apply to the proposed transaction or arrangement, then no such transaction or arrangement may take place and the case should be escalated to the relevant Executive Dean or Professional Services Director, who shall notify the Chief Financial Officer and the General Counsel and Director of Governance and Compliance.

c) If it is determined that there **are no** sanctions which apply to the proposed transaction or arrangement, the check can be signed off by the Line Manager (or equivalent) of the PS staff member who completed the check.

4.4.3.3 Broadly Restricted Countries (BRCs)

a) For any proposed transaction or arrangement between a staff member or the University and an individual or entity based in, or with links to, a Broadly Restricted Country (BRC), a nominated member of the responsible Professional Services (PS) Division should complete a sanctions check in accordance with the Sanctions Assessment Procedure document.

b) If it is identified that there **are** sanctions which apply to the proposed transaction or arrangement, then no such transaction or arrangement may take place and the case should be escalated to the relevant Executive Dean or Professional Services Director, who shall notify the Chief Financial Officer and the General Counsel and Director of Governance and Compliance.

c) If it is determined that there **are no** sanctions which apply to the proposed transaction or arrangement, the check must be escalated to a panel which includes the relevant Executive Dean or Professional Services Director, the Chief Financial Officer, and the General Counsel and Director of Governance and Compliance (or their nominees where required). Depending on the nature of the proposal, it may be necessary to include other appropriate staff on the panel, for example, the Director of Research and Innovation for research collaborations.

d) If the panel decide to approve the assessment, they should consider whether any appropriate mitigating actions need to be put in place to ensure that the proposed activity does not, and is not likely to, fall within the scope of sanctions. This could include a requirement that the relevant team reports on any changes in scope of activity or on any changes in personnel at the University's counterparty.

4.4.4 US sanctions

4.4.4.1 US sanctions apply more broadly than UK sanctions and can sometimes apply to persons in the UK. All US persons, wherever located in the world, are obligated to comply with US sanctions. In addition, US sanctions apply to companies and other entities organised under US law, all branches of US companies and other entities throughout the world, and certain US-origin goods and technology. Therefore, checks for US sanctions are incorporated into the University's sanctions checking process (see Sanctions Assessment Procedure document) and are complied with where applicable.

4.4.5 Storing assessments

4.4.5.1 Evidence of sanctions checks and approvals must be stored appropriately, in line with the Sanctions Assessment Procedure, and the central Sanctions register must be updated.

4.5 **Fraud**

4.5.1 Fraud is a broad and widely used term to describe a number of activities, including theft, false accounting, misappropriation, bribery, corruption, deception, fraud by false representation, including to third parties and collusion. For the purposes of this policy, fraud is defined under relevant legislation and common law and includes any action deliberately designed to cause loss to the University or third parties, or to obtain any unauthorised benefit, whether or not this is received personally or by others. Fraud is considered to be deliberate, rather than a result of unintentional error.

4.5.2 This policy does not apply to fraud with academic implications, as these are addressed by the University's Academic Misconduct procedures. It also does not apply to non-financial employment fraud, e.g. falsification of references, as these are addressed via the University's Disciplinary procedure.

4.5.3 The University is particularly concerned with fraud in the context of financial irregularity. The main types of financial irregularity are the following:

- Theft: including the removal and/or misuse of funds, assets, or cash.
- False accounting: dishonestly destroying, defacing, concealing, or falsifying any account, record, or documents required for any accounting purposes, with a view to personal gain or gain for another, or with the intent to cause loss to the University or subsidiary, or furnishing information which is or may be misleading, false, or deceptive.
- Abuse of position: where fraud is committed by a person or people by virtue of their position or authority, where they are expected to safeguard the University's financial interests or not act against those interests.

Specific examples of these types of financial irregularities within the University context can be found in the supporting documentation.

4.5.4 The fraud prevention framework put in place by the University is informed by the following six principles: i) top level commitment, ii) risk assessment, iii) proportionate risk-based prevention procedures, iv) due diligence, v) communication (including training) and vi) monitoring and review.

4.6 **General Principles**

4.6.1 The University is committed to probity and good conduct in carrying out its business functions and has a zero-tolerance approach to fraud, bribery and any form of dishonesty in its transactions. Any suspected or actual deliberate misconduct outlined within this policy will be subject to a robust investigation.

4.6.2 All members of the University community are expected to behave in a fair and honest way in any internal and external dealings related to the institution.

4.6.3 The University has put internal controls, procedures, policies, and regulations in place to ensure full financial compliance with regard to the law and ethical business standards (particularly given the University's charitable status and receipt of public funding) and those requirements and standards must be followed.

4.7 **Training**

4.7.1 All those covered by the policy must complete all required mandatory financial training offered by the University, which may vary dependent on role.

4.8 **Reporting & Raising Concerns**

4.8.1 Where there is suspicion that fraud or corruption has occurred, or is about to occur, then it is essential that the matter is reported immediately to the Chief Financial Officer. Where that is not possible or appropriate, then the matter should be reported to the Chief Operating Officer, the Vice-Chancellor or the Provost.

4.8.2 Staff should feel empowered to raise specific types of serious concern in good faith without fear of receiving detrimental treatment as a result. The Raising Concerns process can be used to disclose breaches of this policy that fall within the scope of the Public Interest Disclosure Policy.

4.8.3 A suspected breach of sanctions laws, must be immediately reported to all of the following:

- The relevant approver/s of the risk assessment;
- The Chief Financial Officer; and
- General Counsel and Director of Governance and Compliance.

The Chief Financial Officer will subsequently report the breach, if it is confirmed as such, to:

- In respect of financial sanctions, the Office of Financial Sanctions

Implementation (OFSI);

- In respect of trade sanctions: HM Revenue and Customs (HMRC);
- Relevant external stakeholders e.g. Barclays bank;
- The school or division which holds the arrangement; and
- The individual(s) involved.

4.9 **Breach of this policy**

4.9.1 Participation in, or failure to report knowledge or suspicions of, any of the activities outlined in policy which constitute criminal offences are considered to be breaches of this policy.

4.9.2 Where there is deliberate misconduct or behaviour amounting to a wilful breach of this policy, or gross negligence causing a breach of the policy, the matter may be considered under the University's Disciplinary Procedure under Regulation 31.

5. LEGISLATION AND GOOD PRACTICE

Legislation available from https://www.legislation.gov.uk/

5.1 The Bribery Act 2010

5.2 The Criminal Finances Act 2017

5.3 The Proceeds of Crime Act 2002

5.4 Money Laundering Regulations 2017

5.5 The Terrorism Act 2000

5.6 The Sanctions and Anti-Money Laundering Act 2018

5.7 The Fraud Act 2006

5.8 The Economic Crime and Corporate Transparency Act 2023

Good practice and other external guidance:

5.9 British Universities Finance Directors Group Counter-Fraud resources (login required) : BUFDG

5.10 Economic Crime and Corporate Transparency Act 2023: Guidance to organisations on the offence of failure to prevent fraud: Economic Crime and Corporate Transparency Act 2023: Guidance to organisations on the offence of failure to prevent fraud (accessible) - GOV.UK

5.11 UK financial sanctions general guidance: UK financial sanctions general guidance - GOV.UK

5.12 UK trade sanctions general guidance: Trade sanctions, arms embargoes, and other trade restrictions - GOV.UK

5.13 UK sanctions by regime: https://www.gov.uk/government/collections/uk-sanctionsregimes-under-the-sanctions-act

5.14 UK proscribed organisations: https://www.gov.uk/government/publications/proscribed-terror-groups-ororganisations--2

5.15 UK Dept of Trade Goods Checker: OGEL and Goods Checker Tools

5.16 USA Department of Commerce List of Parties of Concern: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern

5.17 USA Office of Foreign Assets Control – Sanctions Programs and Information: https://www.treasury.gov/resource-center/sanctions/

Review / Contacts / References

Policy title:	Financial Compliance Policy
Date approved:	3 July 2026
Approving body:	Council
Last review date:	N/A – first version
Revision history:	Version 1: July 2026
Next review date:	3 July 2029
Related internal policies, procedures, guidance:	Anti-Bribery Procedures / Guidance [TBC] Anti-Money Laundering Procedures / Guidance [TBC] Gifts & Hospitality Sanction Procedures / Guidance [TBC] Sanctions Assessment Procedure [TBC] Fraud Guidance [TBC] Other Finance Policies Public Interest Disclosure Policy Raising Concerns Fraud Response Plan
Division:	Finance
Policy Owner:	Jacinda Humphry, Chief Financial Officer, Finance
Point of Contact:	Sian Thomas, Deputy Director of Finance, Finance