ANTI- MONEY LAUNDERING, TERRORIST FINANCING, AND SANCTIONS (AMLTFS) POLICY

Document record

Maintained by:	Governance and Secretariat
Approved by	Finance Committee
Approval date:	November 2023
Next review by:	November 2026 (or sooner as outlined at paragraph 13)
Location of master document:	LINK

Version control

Document version	Amendments	Date
1.0	N/A	November 2023

ANTI- MONEY LAUNDERING, TERRORIST FINANCING, AND SANCTIONS (AMLTFS) POLICY

1. INTRODUCTION

1.1 The Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000 impose obligations on the University in respect of money laundering and associated activities.

1.2 The University does not consider that it is within scope of the Money Laundering, Terrorist Financing and Transfer of Fund (Information on the Payer) Regulations 2017 (MLRs). The University is not a "relevant person" for the purposes of the MLR, in particular, the University does not come within the MLRs definition of a "financial institution"[1]. This broadly means the University is not subject to the enhanced MLR obligations.

1.3 The University takes money laundering and associated activities very seriously. While the University is not a "relevant person", the University and those identified in paragraph 2.1 (scope of the policy) are still required to comply with the duties imposed by relevant money laundering, terrorist financing and sanctions obligations.

1.4 The law concerning AMLTF is very complex. References to legislation in this policy are summaries only, they are not comprehensive descriptions of the law or the effect of the law. This document should not be relied on as providing legal advice.

2. SCOPE OF THE POLICY

2.1 This policy applies to all staff and associated persons (anyone acting on behalf of the University), including (but not limited to):

2.1.1 employees and workers (whether casual, temporary, fixed-term, permanent or on open-ended contracts), agency workers, seconded workers, volunteers or interns; and

2.1.2 associated persons, including (but not limited to):

2.1.2.1 agents, contractors, associates, consultants, third-party representatives and business partners, suppliers, donors, sponsors, or any other person associated with the University wherever located;

2.1.2.2

[1] See section 10(2) MLR.

2.1.2.3 external members of Council and University committees, panels or boards if they perform services for or on behalf of the University;

2.1.2.4 researchers and academic visitors whether self-funded or employed by other entities (such as other funders, universities or colleges), and retired members of staff, if they perform services for or on behalf of the University;

2.1.2.5 University subsidiary companies and joint venture entities where the University wholly owns or controls the entity unless separate policies have been formally approved and adopted by the Boards of those companies and endorsed by Council. This covers the joint venture partners and, where applicable, those companies conducting services on behalf of the joint venture; and

2.1.2.6 students (i.e. anyone who has a contract for study with the University) when employed by or otherwise acting on behalf of the University, e.g. as members of committees or when representing the University in sports or other competitions.

3. AIMS OF THE POLICY

3.1 This policy intends to:

3.1.1 provide an overview of key offences under anti-money laundering, terrorist financing, and sanctions legislation;

3.1.2 ensure the University and those identified in paragraph 2.1 (scope of the policy) comply with the duties imposed by relevant money laundering, terrorist financing and sanctions obligations;

3.1.3 assist those identified in paragraph 2.1 (scope of the policy) to avoid personal criminal liability;

3.1.4 outline who is responsible for AML compliance at the University; and

3.1.5 ensure steps are taken to avoid, prevent and detect money laundering and terrorist financing breaches in the conduct of the Universities business and activities.

3.2 Breach of this policy by a member of staff of the University may result in an investigation under the University's disciplinary procedures. This may result in disciplinary action, including dismissal.

4. PROCEEDS OF CRIME ACT 2000

4.1 The explanatory notes to POCA define "money laundering" as "*the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently or recycled into further criminal enterprises*". In 2002, money laundering offences were consolidated by POCA, which was the first piece of legislation in the UK to criminalise money laundering in relation to the proceeds of *all* criminal activity, however trivial.

4.2 Broadly, there are three categories of money laundering offences created by POCA:

4.2.1 primary money laundering offences **(sections 327 to 329 POCA**):

4.2.2 secondary money laundering offences (**sections 330 and 331 POCA**) concerned with failures to disclose; and

4.2.3 tipping off and prejudicing an investigation offences (**sections 33A and 342 POCA** respectively).

4.3 The **primary money laundering offences** apply to everyone in the country, whether in an individual or professional capacity, whether or not acting in the "regulated sector" (see paragraphs 4.10 below). The primary money laundering offences carry a maximum penalty of 14 years imprisonment and/ or an unlimited fine on conviction.

4.4 The primary offences are as follows:

4.4.1 **Section 327 POCA** – concealing, disguising, converting, transferring criminal property or removing criminal property from the UK.

4.4.2 **Section 328 POCA** – entering into or becoming concerned in an arrangement which a person knows or suspects facilities (by whatever means) the acquisition, retention, use or control of criminal property, by or on behalf of another person.

4.4.3 **Section 329 POCA** – acquiring (except for adequate consideration), using or possessing criminal property.

4.5 The definition of "criminal property" in POCA is extremely broad. Property is considered criminal property if the following two limbs are met:

4.5.1 It constitutes a person's benefit from criminal conduct, or it represents such a benefit (in whole or in part and whether directly or indirectly), **and**

4.5.2 The alleged offender knows or suspects that it constitutes or represents such a benefit.

4.6 There is no limitation on the amount of money or level of conduct that may lead to prosecution under POCA.

4.7 The **secondary money laundering offences** apply only to persons working in a business in the "regulated sector" (see paragraph 4.10 below).

4.7.1 **Section 330** creates an offence where a person working in a business in the regulated sector, knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in an offence under sections 327 to 329 POCA (the primary offences) but **fails to disclose** that knowledge or suspicion to a "relevant officer".

4.7.2 **Section 331 POCA** creates an offence where a person nominated to receive disclosures under section 330 POCA and working in the regulated sector, knows or suspects or has reasonable grounds to know or suspect money laundering as a consequence of his role of person nominated to received disclosures under section 330, and **fails to make the necessary disclosure** (in accordance with section 338) as soon as practical after the information comes to them.

4.8 **Tipping Off**: Under section 333A POCA, a person working in a business in the regulated sector knows or suspects that another person's suspected involvement with money laundering is under investigation or in contemplation of investigation, and regardless makes a disclosure to any person likely to prejudice any investigation.

4.9 **Prejudicing an investigation**: Finally, Section 342 POCA, prejudicing the investigation, may be committed by individuals in both the regulated and non-regulated sector. Section 342 provides that where a person knows or suspects that a money laundering investigation has, or is about to be, commenced in respect of another and he makes a material disclosure to any other person which is likely to prejudice the investigation, or interferes with relevant materials, commits an offence.

4.10 Again, the offences at sections 330, 331 and 33A POCA may only be committed by individuals in the regulated sector, however, for completeness they have been outlined above. A full definition of what constitutes work in the "regulated sector" is set out in Schedule 9 of POCA. Broadly, this work relates to financial activity (for instance, the work of financial institutions, tax advisors, auditors and accountants, lawyers and notaries, company secretarial services, estate agents etc) and is therefore unlikely to be relevant to employees of the University. Please note that the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 also apply to those in the regulated sector and impose, amounts other things, client identification and record

keeping requirements. As set out above at paragraph 1.2, the University does not consider it falls within the scope of the MLR2017.

4.11 However, if you consider you are carrying out activity in the regulated sector or have any concerns about this, you and your line manager should consult the University Secretary & General Counsel immediately.

5. EXEMPTIONS & DEFENCES AVAILABLE UNDER POCA

5.1 All three primary money laundering offences share a defence. Each of the primary money laundering offences provide that an offence is not committed where an "authorised disclosure" (under section 338 POCA) is made, and "appropriate consent" (defined at section 335 POCA) is obtained. Therefore, no primary money laundering offence will be committed, provided that, before the prohibited act that could trigger commission of the offence is done, an authorised disclosure is made, and consent is obtained from the National Crime Agency (see paragraph 5.4 below).

5.2 Section 337 POCA provides an exemption to persons who receive information in the course of his trade, profession, business or employment, from any legal or other obligation that would otherwise prevent him from making disclosures to the authorities. The required disclosure for the secondary money laundering offences (section 330 (POCA) is a protected disclosure under section 337 to a nominated officer or the National Crime Agency. The explanatory notes of POCA confirm that the protection "*extends not just to the regulated sector which is required to make disclosures in order to avoid committing an offence under section 330, but also to those carrying out any trade, profession business or employment, even if this is not in the regulated sector, who voluntarily make disclosures about money laundering to the police*".

5.3 Section 338 POCA sets out the circumstances in which a disclosure will be "authorised" for the purposes of affording a defence to the principal money laundering offences outlined above (sections 327 to 329 POCA). Where a disclosure is "authorised" for these purposes, there is not to be taken to be a breach of any rule which would otherwise restrict that disclosure. The explanatory notes to POCA explain that "*this is necessary because, in the course of their business, those working inside or outside the regulated sector may need to complete a transaction that they know or suspect could constitute one of the three principal money laundering offences*".

5.4 Once a disclosure has been made to the NCA, it has seven working days to respond to it (excluding the day of receipt). If the NCA does not respond within that period, then a defence

against money laundering (DAML) is afforded to the reporter. If the NCA does respond, it may give a DAML or impose a moratorium period which is initial for 31 days. The NCA may make an application to court to extend the 31- day period, in 31-day increments, for a period of up to six months. During the moratorium, no further steps may be taken without the NCA's consent.

5.5 Other defences may be available depending on the circumstances but details are outside the scope of this policy document.

5.6 Where you know or suspect that a money laundering activity is taking or has taken place, you must follow the University's internal procedure outlined at paragraph 11 (internal reporting procedure) below.

6. TERRORISM FINANCING LEGISLATION

6.1 The Terrorism Act 2000 (TA 2000) is the key piece of legislation in relation to terrorist financing. The TA 2000 criminalizes both the participation in terrorist activities and providing monetary support for such activities. The primary offences are summarised as follows:

6.1.1 **Section 15 – fundraising** is an office if you have knowledge or reasonable cause to suspect that the money or other property may be used for terrorist purposes.

6.1.2 **Section 16 – use and possession** of money or other property for terrorist purposes is an offence if you have reasonable cause to suspect that it may be used for these purposes.

6.1.3 **Section 17 – becoming concerned in funding arrangements** which make money or other property available to another where you know, or have reasonable cause to suspect, that it may be used for the purpose of terrorist activities, is an offence.

6.1.4 **Section 17A** – provides that an insurer commits an offence if they make a payment under an **insurance contract** for money or property handed over in response to a demand made wholly or partly for the purposes of terrorism, when the insurer knows or has reasonable cause to suspect that the money has been handed over for that purpose.

6.1.5 **Section 18 - Money laundering** – it is an offence to facilitate the retention or control of terrorist property by concealment, removal from the jurisdiction, transfer to nominees or in any other way.

6.2 Section 63 TA 2000 also provides that if a person does anything outside the UK and his actions would have constituted the commission of an offence under any of section 15 to 18 TA 2000 had they been done in the UK, they he shall also be guilty of an offence.

6.3 As with POCA, there are secondary offences in relation to failing to make a disclosure or cooperate with the police as well as tipping off (regulated sector only). Section 19 TA 2000 requires business to report any suspicion they may have that someone is committing any of the primary terrorist property offences in sections 15 to 18 TA 2000. Section 20 ensures that businesses can disclose information to the police without fear of breaching other legal restrictions. Section 21 provides a defence to an offence under any of sections 15 to 18 where a person is acting with the express consent of a constable or where a person has disclosed to a constable his suspicion or belief that the money or other property concerned is terrorist property as well as the information which that suspicion or belief is based as soon as is reasonably practicable.

6.4 **Where you know or suspect that a terrorism financing activity is taking or has taken place, you must follow the University's internal procedure outlined at paragraph 11 (internal reporting procedure) below.**

7. SANCTIONS

Overview

7.1 Sanctions are restrictions put in place by the United Nations, UK and other jurisdictions including the United States and European Union, to achieve a specific foreign policy or national security objective. Essentially, sanctions prohibit UK organisations from transacting with particular individuals, bodies or countries that are sanctioned with the aim achieving a foreign policy or national security objective for instance, to restore international peace or fight terrorism.

7.2 There are a number of types of sanctions that the UK may impose including: trade sanctions, financial sanctions, immigration sanctions (i.e. travel bans), and aircraft and shipping sanctions. This policy focuses on financial sanctions. Financial sanctions typically take the form of:

7.2.1 Targeted asset freezes e.g. those that prevent targets moving money, assets or economic resources.

7.2.2 Restrictions on financial markets and services i.e. prohibition of banking relationships, investment bans and restrictions on access to capital markets. In this regard, the University must comply with bank it interacts with including its policies with respect to financial transactions with high risk and/or sanctioned individuals, entities and countries.

7.2.3 Directions to cease all business i.e. these sanctions will specify the type of business and can apply to a specific person, group, sector or country.

7.3 The United Kingdom imposes financial sanctions on individuals or entities rather than on countries or states[2]. This is done through a process of "designation". The Office for Financial Sanctions Implementation ("**OFSI**"), which is part of HM Treasury, maintains a list of individuals and entities that are subject to sanctions. The list details the person's name, pseudonyms and why they are included on the list. See also the lists maintained within the guidance document in paragraph 7.4 below. Lists are dynamic and changed frequently therefore one must always refer to the current list. Additionally, sanctions imposed by the United States of America have extra-territorial reach. This has two main consequences: US authorities have pursued non-US nationals for sanctions breaches; and banks operating in the USA are required to observe US sanctions law in their international operations. The University may therefore be subject to obligations imposed by its bankers reflecting the US sanctions regime. The Office of Foreign Assets Control ("**OFAC**") of the US Department of the Treasury administers and enforces US sanction programs. OFAC maintains list[3] of all active sanction programs.

7.4 The UK Government provides General Guidance for Financial Sanctions Under the Sanctions and Anti-Money Laundering Act 2018[4] (the "**Sanctions Guidance**"). This document is regularly updated and provides information on the approach that OFSI takes to financial sanctions including sector and regime specific guidance and information on monetary penalties for breach of financial sanctions.

Sanctions Offences

7.5 In broad terms, it is a criminal offence to:

7.5.1 breach financial sanctions imposed on a designated person;

7.5.2 circumvent, or attempt to circumvent, financial sanctions imposed on an designated person;

7.5.3 make funds or assets available to designated person (see below for information on designated persons and licensing);

7.5.4 dealing with frozen funds or economic resources (except where an exception applies or under a licence).

This is not an exhaustive list of offences.

Who must comply with financial sanctions?

7.6 The Sanctions Guidance confirms at paragraph 1.4 that:

[2] The primary legislative route through which sanctions are imposed is through regulations made under the Sanctions and Anti-Money Laundering Act 2018, But several other Acts and statutory instruments .
[3] Sanctions Programs and Country Information | Office of Foreign Assets Control (treasury.gov)
[4] Financial sanctions: guidance - GOV.UK (www.gov.uk)

"*UK financial sanctions apply to all persons within the territory and territorial sea of the UK and to all UK persons, wherever they are in the world. This means that: All individuals and legal entities who are within or undertake activities within the UK's territory must comply with UK financial sanctions that are in force. All UK nationals and legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place*."

Exceptions & Licensing

7.7 There are specific exemptions and licensing powers contained in legislation which can allow a designated person to engage in what would otherwise be prohibited. If a sanction states that it is subject to an exception, the exception applies automatically, and it is not necessary to apply for a licence. If there are no stated exception, OFSI may issue a licences to allow defined activity that would otherwise be prohibited by the sanction.

7.8 Where a licence is required, written permission from the OFSI must be sought before the activity is engaged in. It should not ever be assumed that a license will be granted, and no one should engage in any activities prohibited by financial sanctions unless they first have a valid licence.

Reporting

7.9 Under UK legislation, reporting obligations apply to relevant firms (as defined in the UK regulations). The University is not a "relevant firm".

7.10 What constitutes a "relevant firm" will be in the "Information and records" section of each statutory instrument for each sanctions regime. However, guidance[5] confirms that examples include the following:

7.10.1 a person that has permission under Part 4A of the Financial Services and Markets Act 2000 (FSMA 2000) (Permission to carry on regulated activities)

7.10.2 an undertaking that by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means, or cashes cheques which are made payable to customers

7.10.3 a firm or sole practitioner that is a statutory auditor or local auditor

7.10.4 a firm or sole practitioner that provides by way of business accountancy services, legal or notarial services, advice about tax affairs or certain trust or company services

5

7.10.5 a firm or sole practitioner that carries out, or whose employees carry out, estate agency work

7.10.6 the holder of a casino operating licence

7.10.7 a person engaged in the business of making, supplying, selling (including selling by auction) or exchanging articles made from gold, silver, platinum, palladium or precious stones or pearls.

7.10.8 a cryptoasset exchange provider

7.10.9 a custodian wallet provider

7.11 Relevant firms are required to inform OFSI as soon as practicable if they know or reasonably suspect a person is a designated person or has committed offences under financial sanctions legislation. This requirement applies to relevant firms in the UK or under UK jurisdiction, including individuals working for them.

What am I required to do?

7.12 Members of staff should familiarise themselves with University Guidance on Receiving Payments from Sanctioned Countries. This guidance sets out a process relating to the receipt of tuition fees from students and sponsors. In addition, the University's procurement team will carry out reviews of suppliers and the University's banks also check some payments received. Any one of these measures or actions could result in a payment being flagged. The University's Code of Practice for the Acceptance of Donations also prohibits the acceptance of donations from individuals or entities subject to sanctions.

7.13 The University's travel insurer must pre-approve travel to a list of territories, which is consistent with territories in which individuals and entities have been designated. Prior to travelling to these territories, members of staff must obtain permission from their line manager; carry out a risk assessment having taken advice from the University's Health, Safety and Environment Team, competed the necessary training and familiarised themselves with the content of and complied with the University's Health and Safety and Employee Travel & Expenses policies.

7.14 **Accordingly, where you know or reasonably suspect that a person is a designated person (a designated person is an individual, entity or ship, listed under UK legislation as being subject to sanctions, see lists referred to in paragraph 7.3 above) or there has been an offence under any applicable sanctions law, you must first cease all activity with that person and report this immediately to: the Chief Financial Officer.** Note that you must not return any money paid or deliver any services to the person: you must simply stop all activity and make the report to the Chief Financial Officer.

7.15 Where appropriate, the Chief Financial Officer must then make a report to HM Treasury's Office of Financial Sanctions Implementation as soon as practicable. Failure to make a report is a criminal offence.

8. RISKS TO WHICH BRUNEL UNIVERSITY LONDON MAY BE EXPOSED

8.1 To counter the risk of becoming accidentally involved in money laundering, the principal risks need to be identified, assessed and procedures put into place to mitigate the risks.

8.2 British Universities Finance Directors Group ("**BUFDG**") guidance suggests that particular care be focused on:

- Payments in cash
- Applicants from high risk countries
- Requests for refunds – (particularly to a different account or individual to the payer)
- Overpayments
- Failure to take up places
- Agents who do not fit in with normal procedures relating to deposits and tuition fees
- Identity fraud

8.3 Normally it would be considered suspicious if a customer purchased a product by overpaying and then requesting the excess be transferred into a different account.

8.4 It could be considered suspicious for a debt to be settled by an independent third party. It is normal for student debt in the form of tuition fees for international students or living expense owed to be settled by a third party (parent) but other instances should be reviewed.

8.5 Criminals have previously targeted universities, and we need to be extra vigilant in this area.

9. STUDENT AND CUSTOMER IDENTIFICATION – "KNOW YOUR CUSTOMER"

9.1 It is important that controls are in place to identify the student, customer or other third party dealing with the University. In the case of students, examples include passport, visa, birth certificate and correspondence with students at their home address. For people who intend to support the student, proofs such as letters or documents proving name, address and relationship with the student are required. If the sponsor for the student is a company, a letter on company headed paper explaining the relationship between the company and the

student and that permission has been given to pay tuition fees or tuition fees plus Brunel accommodation fees by that company.

9.2 For non-student debt, if the organisation is not known to the University, look for letter headed documents, check websites or request credit checks to verify the validity of the potential customer. Cheques drawn from an unusual source should always be investigated.

10. CONTROLS TO MITIGATE RISK

10.1 Maintaining adequate records of transactions. The Finance Retention Schedule delineates the University's record retention policy in respect of category of relevant record. Further information can be obtained by emailing the Records Management Team at recordsmanagement@brunel.ac.uk. **It is important to ensure that relevant notes made are not inappropriately distributed to ensure that a tipping off offence is not inadvertently committed**.

10.2 The University shall provide training to staff on anti-money laundering and reporting policies, particularly for all professional service staff and all student facing staff.

10.3 No cash transactions for payment of tuition fees will be permitted.

10.4 Students will be advised that they are not permitted to pay the fees of another student.

10.5 Refunds of payments made in respect of either student or non-student debt should only be made by the same method and to the same account as the original payment was made.

10.6 In the event of payment by credit or debit card being rejected, the reason should if possible be checked with the card provider prior to accepting an alternative card with different detail.

10.7 Students must make arrangements to cover their living expenses prior to arrival. This includes setting up their bank accounts. If a donor or third party sends funds in excess of requested tuition fees, the excess can either be repaid to the donor using the same bank details or, with the permission in writing of the donor, be used to fund Brunel accommodation due. The excess cannot be transferred to the student.

10.8 Fees paid in advance for foreign students who have subsequently been refused a visa shall be dealt with in accordance with the Student Finance Policy in force at the relevant time.

11. INTERNAL REPORTING PROCEDURE

11.1 When you know or suspect that a money laundering or terrorist financing activity is taking or has taken place you must disclose this immediately to your line manager. If, in consultation with your line manager suspicion is upheld, a disclosure report should be made to the Head of Income. If the initial disclosure was made under the University's Whistleblowing Policy, it may be referred to the Head of Income where appropriate to do so. If the concern relates to activity of the line manager, concerns may be escalated to University officers named in the Whistleblowing Policy.

11.2 The report should contain as much detail as possible including:

- Full available details of the people, companies involved and all staff members who have dealt with the suspected transaction;
- Reasons as to why you are suspicious;
- Dates of the transactions, amounts involved and method of transfer of money or assets;
- Any other information that may help assess the case for knowledge or suspicion of money laundering.

11.3 Once you have reported your suspicions neither you nor your concurring line manager should make any further enquiries nor discuss your suspicions further unless instructed otherwise to avoid making a disclosure which may prejudice a money laundering investigation or amount to a tipping off offence (regulated sector only). You must also stop all work pending receipt of instructions from the individual to whom the report was made as to next steps. Further, bear in mind that if one person internally tells another that a disclosure has been made to the NCA, that may be committing a prejudicing an investigation offence under section 342 POCA.

11.4 The University will support anyone who raises concerns in good faith under this policy, even if any subsequent investigation finds that they were mistaken.

11.5 The University will ensure that no one suffers any detrimental treatment as a result of reporting a concern relating to potential act(s) of money laundering or terrorist financing.

12. ADVICE TO MEMBERS OF STAFF IN IDENTIFYING MONEY LAUNDERING

It is not possible to give a definitive list of ways to spot money laundering. The following are types of risk factors which may be considered:

- A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation;
- Is the customer or student requesting a large cash transaction – especially where the cash is used notes or small denominations;
- Payment of any substantial sum in cash (over £1,000);
- Concerns about the honesty, integrity, identity or location of the people involved;
- Involvement of an unconnected third party without a logical reason or explanation;
- Overpayments for no apparent reason;
- Absence of any legitimate source for the funds received;
- Significant changes in the size, nature, frequency of transactions with a customer that is without reasonable explanation;
- Cancellation, reversal or requests for refunds of earlier transactions;
- Requests for account details outside the normal course of business;
- Requests for payments or refunds after funds have been paid into the University's bank account by a third party;
- A history of poor business records, controls or inconsistent dealing;
- Any other facts which tend to suggest that something unusual is happening and give reasonable suspicion about the motives of individuals.

13. **REVIEW**

This policy will be reviewed:

- every 3 years;
- in the event of a trigger event such as a change in legislation or guidance, the identification of a new or emerging money laundering or terrorist finance risk or changes to relevant systems and process of the University; or
- if there is any other reason to suspect the policy is no longer valid such as a significant change in the matters to which it relates

whichever occurs sooner.

This policy may also be reviewed and updated as required to incorporate learning from instances of money laundering or near misses and changes to the organisation.