

**The Open University And**

**The Open University Student Budget**

**Accounts Limited**

Group Anti-Money Laundering Policy

# SEPTEMBER 2020

**CONTENTS**

|  |  |
| --- | --- |
| A | Background and Statutory Framework |
| B | Risk Based Approach |
| C | Risk Assessment |
| D | Money Laundering Reporting Officer |
| E | Know Your Customer/ Customer Due Diligence |
| F | Reporting Suspicions |
| G | Awareness and Training |
| H | Record Keeping |
| I | Consequences of Breach |
| **APPENDIX** |  |
| I | Risk Assessment Matrix |
| 2 | Client Identification/ Customer Due Diligence |
| 3 | Money Laundering Suspicion Reporting Form |

1. **Background and Statutory Framework**

## Background

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. This is achieved by changing illicit funds into what appears to be legitimately generated money.

In the UK, severe penalties are imposed on individuals connected with any stage of laundering money, including unlimited fines and/or terms of imprisonment ranging from 5 to 14 years for assisting a money launderer, tipping-off a suspected money launderer, or failing to report knowledge or suspicion of money laundering.

It is therefore recognised by us at The Open University (OU) and Open University Student Budget Accounts Limited (a wholly owned subsidiary of the OU (OUSBA)) (“the Group”) that our institution, in so far as it conducts financial services activity, does not become involved either in legitimisation of an individual with a criminal intent or background through provision of its loan facility allowing him/ her an entry into the financial system for a suspect activity or in any transaction that may give rise to a suspicion that it has wrongly assisted or had a business dealing with a money launderer. All members\* representing the Group in any capacity will be responsible for reporting any suspicious transactions to the Money Laundering Reporting Officer (MLRO) or Nominated Officer (NO), as applicable (see section D below for more details).

The relevant staff within the Group will undertake awareness training in anti-money laundering regulations and procedures. A copy of this AML policy and procedures manual is provided to all relevant staff who are likely to deal with the financial services lending/ credit broking activity, to ensure they are aware of their responsibilities under the regulations.

The money laundering rules create a number of criminal offences in respect of assisting money laundering. There are criminal penalties for:

* + Failing to report knowledge or suspicion of money laundering
  + Failing to have adequate procedures to guard against money laundering
  + Knowingly assisting money launderers
  + Tipping–off suspected money launderers

In summary, there are five key requirements arising from the money laundering regulations:

* + All firms must obtain satisfactory evidence of the identity of each customer with whom it deals with and/ or has a business relationship

(\* Members are any relevant employee of the Group, including temporary or part- time, contractor or Appointed Representative, who have any involvement in the OU or OUSBA’s credit related activities)

* + This evidence of client identity must be retained for the duration of the client relationship and for a period of five years after it terminates; details of transactions must be kept for the same time period
  + Any suspicious transaction, whether in connection with a new or existing client, must be reported immediately to the MLRO/ DMLRO or the NO, as applicable.
  + The MLRO must, if deemed appropriate, report suspicion of money laundering to the appropriate authorities; in the UK, this is the National Crime Agency (NCA)
  + Appropriate training must be provided to all relevant members of staff who handle, or are responsible for handling, any transactions with the Group’s clients and counterparties (including prospective customers) to ensure they are aware of Group procedures which guard against money laundering and the legal requirements of the money laundering rules; this training will be co-ordinated by the MLRO/ DMRO/NO.

OU’s and OUSBAs procedures have been designed to ensure compliance with all these requirements on a risk-sensitive basis for prevention of financial crime and money laundering, as detailed in this manual. It is a requirement for all relevant staff members to read the contents of the manual which deals with the Group’s policy and provide a confirmation thereof to the MLRO/ DMLRO/ NO.

## Statutory Framework

The UK approach to fighting money laundering and terrorist financing is based on a partnership between the public and private sectors. Objectives are specified in legislation and in the FCA Rules, but often the objective itself will be a requirement of an EU Directive, incorporated into UK law without any further elaboration, leaving UK financial businesses discretion in interpreting how it should be met.

Key elements of the UK AML framework that applies to the Group are:

* Proceeds of Crime Act 2002 (as amended by Criminal Finances Act 2017);
* Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001);
* Money Laundering Regulations 2017 (as amended);
* FCA’s Handbook rules/ guidance including the Financial Crime Guide for firms
* Counter-terrorism Act 2008, Schedule 7;
* HM Treasury Sanctions Notices and News Releases; and
* Joint Money Laundering Steering Group (JMLSG) Guidance approved by HM Treasury.

# Risk Based Approach

The Money Laundering Regulations 2017 (“the Regulations”), which transposed the EU’s 4th Money Laundering Directive into the UK law, require firms to set out policies and procedures for carrying out customer due diligence, and transaction monitoring arrangements, on a risk sensitive basis. The Regulations place special emphasis on the need for firms to adopt suitable systems and controls to mitigate any financial crime risks to their businesses based on a risk-based approach and require them to demonstrate and document that the risk assessment is carried out and kept up-to-date. The FCA’s Financial Crime Guide places a similar requirement on firms to conduct regular risk assessment of their financial crime risks.

Certain amendments to the Regulations, arising from the provisions of the EU’s 5th Money Laundering Directive (which did not require a formal transposition by UK due to Brexit), have been made to maintain equivalence with the EU legislation with effect from January 2020. Whilst the amendments relating to e-money transactions, safe deposit vaults, beneficial owners of corporate entities and crypto-currencies etc. do not have any impact on the regulated activities of the Group, the new requirement to carry out enhanced due diligence for transactions relating to customers based in high risk third countries (mainly non-EU jurisdictions which do not enjoy an ‘equivalent’ status) could have a potential bearing on the Group’s policy. Currently, OUSBA provides student loans only to the residents within the UK and EU, however, the policy will need to be reviewed to ensure compliance with the new requirements under the Regulations if the lending activity is extended to students residing in such high risk third countries in the future. The Group’s policies and procedures are regularly reviewed and tailored to ensure they take account of the different risks and vulnerabilities, associated with its products and services offered, and its customer base.

Assessments of money laundering risks in terms of the different business areas, products and services provided, and the respective customer bases, should be made by the MLRO/ NO in liaison with appropriate line management to provide reasonable assurance that the Group’s Anti-money laundering policies and procedures will assist in the prevention and detection of money laundering.

In terms of the current regulatory requirements, the Group has adopted a risk based approach to addressing the money laundering/terrorist financing risk faced by our business.

An assessment of the money laundering/terrorist financing risk to the Group’s business has been carried out, having regard to the nature of products and services offered by OU and OUSBA, with a view to designing appropriate controls, in terms of the ‘know your customer’/ ‘Customer due diligence’ information to be collected and verified.

The OU’s activity of introducing prospective students to its affiliate lender for a student loan (which falls within the regulated activity of credit broking) is considered a low risk activity from the perspective of money laundering.

However, all staff need to be vigilant against the financial crime and fraud risks in any business and profession and as such any suspicions arising in the normal course of business must be reported promptly to the MLRO/ NO, for further investigation and external reporting, as required, in terms of the procedures detailed in this manual.

# Risk Assessment

As part of the review of this policy, a further risk assessment of the current product and services provided by the Group has been carried out, as set out below. Both The OU and OUSBA focus their AML controls in proportion to the financial crime risks, including:

* **Product/ Service risk** (risk assessments for our standard product/service types)
* **Party risk** (e.g. customers, beneficial owners, third parties, contractors and agents) including information on Politically Exposed Persons (PEPs) and Sanctioned parties
* **Jurisdiction/Country risk** e.g. countries the Group operates in, or the location of our supplier, agent or customers, or the source or destination of transactions
* **Distribution channel risk** including whether the business is direct, via a third party, face to face or digital/telephone



JMLSG Guidance and FCA’s Financial Crime Guide provide guidelines for assessing the

anti-money laundering risks considering the nature of products/ services, customers,

jurisdiction and distribution channels used by regulated firms as set out below.

### Product and Service features, parties (customers/ suppliers), jurisdictions and

**distribution channel that may increase the financial crime risks for the Group** include:

* **Product, service and distribution channel risk factors**
* Cash or Anonymous transactions
* Non face-to-face business relationships or transactions
* Payment received from unknown or un-associated third parties
* Introductions from unregulated third parties

### Customer risk factors

* The business relationship is conducted in unusual circumstances
* Non-resident customers
* Business that are cash intensive
* Politically Exposed Persons (PEPs) and Sanctioned individuals/ entities

### Country or geographic risk factors

* Countries identified by credible sources as not having adequate AML/CTF approaches
* Countries subject to sanctions, embargoes, or similar measures issued by, for example, the United Nations and HM Treasury
* Countries identified by credible sources as providing support for terrorist activities, or that have designated terrorist organisations operating within their country

Accordingly, an assessment of the Anti-Money Laundering (AML) risks associated with the Group’s products and processes under its current business model/ proposition has been completed. The Group’s updated AML risk assessment takes account of the above factors and assigns three different levels of risk (High, Medium and Low) to each risk factor, as detailed in the attached Risk Assessment Matrix (Appendix 1).

The risk assessment is based on the Group’s current products and processes described below.

#### Product/ Service Risks:

The OU introduces prospective students who need financial assistance for undertaking higher studies to OUSBA. OUSBA currently offers a low interest bearing simple student loan product, which has an inherent ‘low’ AML risk as, due to the very nature of the product, such loan products do not provide the functionalities required for laundering money (ie placement, layering etc.) to criminals. However, there could be potential risks associated with any accelerated and/ or third party payments into the account, especially if such third parties and the source of funds are not known to OU/ OUSBA.

Post-Control

The controls in place for mitigating the AML and fraud risks are set out in this policy. Funds are always paid directly to the student’s course provider (the OU). Third party payments are accepted only from the bank accounts of the parties who have been authorised by the students to make payments on their behalf. In such cases no further due diligence is carried out if the parties making repayment for payments up to £800.

However, additional due diligence will be carried out when payments are made by third parties for an amount exceeding £800 (please see ‘When must identity be verified’ section below) either by way of electronic check of identity with their consent or verifying a documentary proof of identity, as appropriate.

Therefore, post-control product/ service risk for both OU and OUSBA is considered as **‘low’**.

#### Customer Risk

OUSBA’s target customers are residents in either UK or EEA countries and comprise students duly introduced by the OU if they need financial assistance for pursuing and funding the fees for their selected courses. These students are unlikely to fall into any of the ‘high-risk’ categories (however a ‘high-risk’ customer screening is carried out as part of the initial customer due diligence - see below).

Post-control

The Customer Due Diligence (CDD) procedures set out in this policy are designed to mitigate the potential customer risk. Verification of each applicant is carried out by using the standard due diligence procedure and the check for ‘high-risk’ category (‘Sanctions and PEPs’) is carried out prior to the loan being disbursed. While this forms part of the electronic checks conducted for all UK students, the ‘sanctions’ check for non-UK applicants is carried out through a manual verification against the HMT’s updated consolidated list of sanctions published on its website.

A PEP-related AML risk is unlikely to arise in the type of activities undertaken by OU and OUSBA i.e. provision of loans for funding of course fee to prospective students. However, the electronic verification of customers by way of standard due diligence include PEP checks and, where e-verification is not feasible (for non-UK students), a manual ‘google’ search will be carried out to check if there is any PEP link.

A positive PEP or Sanctions match will be referred to the MLRO/NO/ DMLRO for further investigation and advice before proceeding further with the case.

Accordingly, the post-control customer risk for the group is considered as **‘low’**

#### Jurisdiction Risk

The current jurisdiction for all activities is limited to conducting distance learning activities from the UK establishment of the OU. Currently, the Group provides loan facilities only to students from either the UK or EEA/ European jurisdictions. The JMLSG guidance clarifies that a presumption of low risk applies to these jurisdictions unless the firm’s experience with certain types of customers within these jurisdictions calls for a higher risk factor to be applied. The Group experience has not given rise to any particular risks associated with the students from these countries.

The jurisdiction risk associated with provision of such services by the Group is therefore considered as **‘low’**.

#### Distribution Risk

OUSBA’s products are distributed via introductions provided by the Open University (a well- known, reputed learning institution) and both the OU and OUSBA are regulated by the FCA for introducing and lending activities respectively. Even where the OU’s appointed representatives refer students for enrolment to certain courses of study, the referrals to OUSBA for loans are made only by the OU after their staff have followed due process which involves use of pre-approved scripts for making the required disclosures to prospective students. We therefore consider the post-control distribution risk to the group as **‘low’**.

#### Overall Risk

In terms of the risk assessment, the overall (post-control) financial crime ‘risks’ associated with the OU and OUSBA’s product and services have been assigned the risk rating of **‘LOW’**. The rating reflects the systems and controls in place especially in areas where the inherent (gross) risk is either ‘medium’ or ‘’high’. Our controls for mitigation of any potential risks have been set out in this policy, which include the appointment of an MLRO and

DMLRO, other systems and controls and periodic staff awareness training. In addition, the Group has decided to commission an annual external audit to review its systems and controls for AML including validation of the annual risk assessment in light of the customer experience of the Group in conjunction with the latest risk guidance issued by the FCA and JMLSG.

# MONEY LAUNDERING REPORTING OFFICER

In terms of the FCA rules, a firm must:

1. Appoint an individual as MLRO, with responsibility for oversight of its compliance with the FCA’s rules on systems and controls against Money Laundering; and
2. Ensure that its MLRO has a level of authority and independence within the firm and access to resources and information sufficient to enable him to carry out that responsibility.

In accordance with the JMLSG guidance, firms which have no obligation to appoint an MLRO under the FCA rules may nevertheless choose to appoint a Nominated Officer (NO) for administrative convenience and to assist their staff to fulfil their obligations under the FCA’s high-level requirements for managing risks of financial crime, suspicion reporting under the Proceeds of Crime Act 2002 (POCA) or Terrorism Act. The Open University is exempt from the requirement to appoint an MLRO and hence it has nominated a member of its senior management who oversees the credit broking activity as a Nominated Officer (NO) for the purposes of overseeing AML controls of the OU and reporting of any suspicions arising within credit broking business.

The job of the MLRO/ NO within a firm is to act as the focal point for all activity relating to anti- money laundering. The FCA expects a firm’s MLRO to be based in the UK.

The Money Laundering Reporting Officer for OUSBA is Brian Cheyne, Director of Treasury Services. He is also the Nominated Officer (NO) for the OU. Gail Bradford has been designated as the DMLRO for OUSBA and acts as the NO for the OU and MLRO for OUSBA in the absence of Brian Cheyne. She also has the delegated responsibility to receive internal suspicion reports from staff and make external reports to the National Crime Agency, if required, in consultation with the MLRO/ NO, as appropriate.

The above named Officers will also be the conduit for the reporting of Fraud.

# Know Your Customer/ Customer Due Diligence

## The Requirements

The Regulations require that firms must be reasonably satisfied as to the identity of the client (student-applicant), comprising name, permanent address and / or date of birth, as part of their customer due diligence (CDD) processes before commencing a business relationship. The CDD measures involve: (a) identifying the customer, and verifying his identity**;** (b) identifying the beneficial owner, where relevant, and verifying his identity on a risk sensitive basis**;** and (c) obtaining information on the purpose and intended nature of the business relationship. There is a further requirement for firms to conduct ongoing monitoring of the business relationship with their customers as part of their ongoing due diligence.

Identifying a customer is a two-part process. It has been agreed between the OU and OUSBA that OUSBA will undertake the necessary customer identification process before completion of any loan. OUSBA first identifies the student (customer), by obtaining a range of information from him or her. The second part – the verification – consists of OUSBA verifying some of this information through the use of reliable, independent sources of documents, data or information.

How much identity information or evidence to ask for, and what to verify, in order to be reasonably satisfied as to a customer’s identity, are matters for the judgement of the Group, which will be exercised on a risk-based approach, taking into account factors such as:

1. the nature of the product or service sought by the customer (generally it will be for a student loan);
2. the nature and length of any existing or previous relationship between the student and the University (i.e. whether the student has already pursued a course with the OU before);
3. the nature and extent of any assurances from other regulated firms that may be relied on (i.e. if introduced by another regulated entity);
4. whether the student (customer) is physically present.

OUSBA and the OU share premises and so share data between them in order to make the assessment set out above. The Regulations require a risk-based approach to establishing identity, and, accordingly, the higher the perceived risk of potential money laundering activity (e.g. potential client is a resident or national of a designated high risk country), the more stringent the identity verification procedures should be.

## Exemptions from standard CDD requirements

The Regulations have removed the provision relating to automatic exemptions from CDD requirements in situations where verification of identity is generally not required. Firms are required to take a risk-based approach to set out any simplified due diligence process in low risk relationships. The Group will adopt a simplified process for verifying the identity for the following relationships.

1. Client is a credit institution
2. Client is a financial institution covered by the Money Laundering Directive/ Regulations
3. Client is another UK regulated firm that is bound by the FCA sourcebook, the Money Laundering Regulations or is otherwise covered by the Money Laundering Directive
4. Client is introduced by an overseas institution that:
   1. is subject to regulatory oversight exercised by a relevant overseas regulatory authority (within the meaning of section 82 of the Companies Act 1989); and
   2. is subject to legislation at least equivalent to that required by the Money Laundering Directive; and
   3. gives a written assurance that it has obtained and recorded evidence of identity of the client.

Where any prospective client meets any of the above conditions, the staff should refer the case to the Operations Manager who will authorise the acceptance of business relationship based on checking the details of the firm and its authorised directors through publicly available information/ records (such as the FCA register, Company House search etc.) and provide guidance for seeking any other documentary verification, where necessary.

## Standard CDD Requirements for all customers

Identity should be verified for the following categories of clients:

1. Named account holder (all account holders in the case of joint accounts)
2. The principal controllers of an account or business relationship (i.e. those who regularly provide instructions)
3. Any third party making payment on behalf of the customer for an amount exceeding

£800 (see below for further details).

### The specific identification requirements for different categories of clients have been set out in Appendix 2. These requirements must always be adhered (unless the identity is verified electronically as specified in this policy) to and any instance where it has not been possible to comply with them should be immediately brought to the attention of MLRO/ DMLRO for further guidance.

Typically, the originals of the identification document should be seen by a representative or employee of OUSBA, who must take copies thereof and sign and date them in confirmation of having seen and verified the original. This information will then be stored and shared with the OU. The Joint Money Laundering Steering Group (JSMLG) have recommended against requesting originals of valuable personal identity documents (e.g. passport, identity card, driving license) by post, in order to guard against postal interception and fraud. In the case of non-face-to-face contact for UK residents, copies of documents can be certified by an ‘appropriate person’, that is, someone in a position of responsibility (such as a representative of an FCA authorised firm, lawyer, accountant etc) who knows or has met with the customer, and may reasonably confirm the customer’s identity.

## When must identity be verified?

Whenever a business relationship is likely to be established, identification evidence must be obtained. The Group will ensure that the identity of all applicants is verified before any loan completes. The identity of any third parties making payments on behalf of the customer will also be checked if a payment in excess of £800 to ensure compliance with the provision under the Regulations which requires customer due diligence to be applied (on a risk-sensitive basis) for an occasional transaction for an amount exceeding 1,000 Euros.

Once identification procedures have been satisfactorily completed and the business relationship has been established, as long as contact or activity is maintained and records concerning that customer are maintained, no further evidence of identity is needed when transactions or activity are subsequently undertaken (except to ensure the transaction is bona fide and for the stated customer). Both OU and OUSBA (who are related companies as set out above) will share data as necessary in order to ensure the requirements of this policy are met

## Identity of private individuals

The Group should obtain the following information in relation to a personal customer:

* + full name
  + residential address
  + date of birth

If documentary evidence of an individual’s identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned.

In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the Group reasonable confidence in the customer’s identity, although the Group should weigh these against the risks involved.

If identity is to be verified from documents, this is normally based on:

*Either* a government-issued document which incorporates:

* + the customer’s full name and photograph, and either
  + his or her residential address, or
  + his or her date of birth.

e.g.:

* + Valid passport
  + Valid photocard driving licence (full or provisional)
  + National Identity card (non-UK nationals)
  + Firearms certificate or shotgun licence
  + Identity card issued by the Electoral Office for Northern Ireland

*or* a government-issued document (without a photograph) which incorporates the customer’s full name, supported by a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, or another FCA-regulated firm in the UK financial services sector, or in a comparable jurisdiction, which incorporates:

* + the customer’s full name and either
  + his or her residential address, or
  + his or her date of birth

e.g.:

1. Government-issued documents without a photograph include:
   * Valid (old style) full UK driving licence
   * Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant
2. Other documents include:
   * Instrument of a court appointment (such as liquidator, or grant of probate)
   * Current council tax demand letter, or statement for the current year
   * Current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK, EU or comparable jurisdiction (but not ones printed off the internet)
   * Utility bills (but not ones printed off the internet) less than three months old

The above procedure for identifying customers will meet the requirements of standard due diligence.

For all UK applicants, it is the policy of the Group to undertake client identification by way of electronic verification through a credit check by using one of the three accredited Credit Reference Agencies in the UK. If the name and/ or address of the applicant cannot be confirmed electronically, a manual verification is carried out by seeking required paper documentation from lists A and/ or B, as applicable (see Appendix 2).

Considering the provisions of the Financial Sanctions regime of HM Treasury, each applicant should be checked against the updated list of financial sanctions available on the HMT’s website. These checks can be performed through the electronic verification process for the UK applicants.

In respect of the applicants from EEA states where a national identity card (or a similar document) is issued by the government agencies to their citizens, which contains verified details of the individual’s name, date of birth and address, a copy of that document will suffice for the purpose of both name and address checks without the need for any further verification. However, where such a document is not available, suitable alternative documents from lists A and B in Appendix 2 (as issued in the relevant EEA country) should be requested. If a customer is unable to provide any of the listed documents, the case should be referred to the MLRO/ DMLRO for further guidance.

## Suitable Alternative Electronic Verification

JMLSG guidance states that firms will usually need to be prepared to accept a range of documents and other available tools to verify customer identity, and it expressly allows firms to employ electronic checks, either on their own or in combination with documentary evidence.

Accordingly, the identity and address of its customers can be verified by OUSBA by way of electronic verification process which satisfies pre-agreed criteria detailed, either on its own or in conjunction with documentary verification. Electronic checks should be carried out by employing an accredited e-verification mechanism which uses multiple data sources from authentic sources across time (such as the Voter’s Roll, Shared Database from the UK

financial institutions, passport checks etc) providing the verification produces a satisfactory level of corroboration of the data supplied by the customer by meeting the matching criteria specified by the Group. The documentary evidence can, however, be resorted to as a secondary and additional check, if required following the initial electronic verification, if the electronic evidence on its own does not provide required standards of verification of the customer’s identity.

## Non face-to-face identification and verification

Non face-to-face identification and verification carries an inherent risk of impersonation or fraud. Where identity is verified electronically, or copy documents are relied on, the Group should apply an additional verification check to manage the risk of impersonation/ fraud. The additional check may consist of measures, such as:

* + requiring the first payment to be carried out through an account in the customer’s name with a UK or EU regulated credit institution or one from a comparable jurisdiction
  + verifying additional aspects of the customer’s identity, or of his or her electronic ‘footprint’
  + communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration)
  + internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up for them and provided by mail (or secure delivery) to the named individual at an independently verified address
  + requiring copy documents to be certified by an appropriate person.

## Certifying paper identity documents (where electronic verification cannot be completed)

For Non-UK applicants, where copies of any paper documents are requested, these should be certified by an appropriate person. A certification by a professional person such as a bank official, councillor, solicitor, notary, doctor/ dentist, accountant, teacher, an official of the Embassy/ High Commission or by an Appointed Representative of the OU will be acceptable for this purpose. Any representative of the OU or OUSBA can also certify the documents if they have an opportunity to meet the students prior to the loan completion.

However, if the certification of the identity document proves difficult (or does not appear to be a cost or time effective option for the student), a copy of the bank statement (dated within last 3 months) will be requested as an additional document to verify the name and address of the customer. The statement should relate to the account from which the student proposes to make loan repayments (by Direct Debit) and the bank is a UK/ EU institution.

### In summary:

#### For UK students, an electronic verification of identity (including screening against the HMT Sanctions/ PEP list) is carried out by OUSBA. Failure to confirm the identity electronically triggers a manual process as set out above.

1. ***For non-UK/ EEA applicants, a certified copy of the national ID card (or an equivalent document) is requested. In case of any difficulties in getting certified document, an additional document by way of a bank statement (dates within last 3 months) relating to the account to be used by the applicant for making ‘direct debit’ payments is called for. Use of two documents is designed as an additional measure to mitigate the fraud-risk where uncertified documents are provided.***

Also, in all instances where the identity is verified non-electronically, the check against the HMT’s Sanctions/ PEP will be required to be carried out manually.

Staff members will refer any cases that do not satisfy standard requirements to the DMLRO/ NO.

# Reporting Suspicions

The Group takes reasonable steps to ensure that:

1. Any member of staff who handles, or is responsible for handling, transactions which give rise to suspicions of money laundering must make a report promptly to the MLRO/DMLRO/ NO if he or she knows or suspects that a client, or the person on whose behalf the client is acting, may be engaged in money laundering.
2. Action will be taken to discipline any member of staff who fails, without reasonable grounds, to make a report of the kind envisaged in this section.

Once an employee has reported his/her suspicion to the MLRO/ DMLRO/NO, he/she has fully satisfied their statutory obligation.

## Internal Reporting Procedures

### Reporting Suspicious Activity

All members are required to report any instances of suspicions promptly to MLRO/ DMLRO/ NO for which they can use the format provided at Appendix 3 to this policy manual. All suspicions reported to the MLRO/ DMLRO/ NO must be documented (in urgent cases this may follow an initial discussion), which can also be done by sending an email to the MLRO/ DMLRO/ NO. If reports are made by telephone, it is important that the MLRO/ DMLRO/ NO provides the documentary report and that the full name of the member of staff and department be recorded.

### Reporting High-Risk Customer matches

Staff members must also report a customer to the MLRO/ DMLRO if the result of Sanctions match is returned as positive either as part of electronic checks on any UK applicants or manual checks on non-UK applicants and should follow his/ her advice and guidance before proceeding further with the processing of the loan application. And though there is no apparent PEP risk associated with the Group products, a positive PEP match, if any, should also be referred to the MLRO/ DMLRO for and any further check and/or guidance for monitoring purposes, if necessary.

## External Reporting Procedures - Regulatory Requirements

All internal reports must be considered by the MLRO/ DMLRO/ NO in the light of all other relevant information for the purpose of determining whether or not there is knowledge or suspicion of money laundering. Where following consideration such knowledge or suspicion remains, a report must be made to National Crime Agency (NCA).

The firm must take reasonable steps to ensure that an internal report of suspected money laundering is considered by the MLRO/ DMLRO/ NO and that having considered the report and any relevant know your business information to which he has sought access, the MLRO/ DMLRO/ NO suspects that a person has been engaged in money laundering, he/she reports promptly to NCA.

To take reasonable steps, the firm should:

* 1. require that the MLRO/ DMLRO/ NO considers a report in the light of all relevant information accessible to, or reasonably obtainable by them;
  2. permit the MLRO/ DMLRO/ NO to have access to any information, including know your business information in the firm’s possession which could be relevant; and
  3. ensure that where the MLRO/ DMLRO/ NO suspects that a person has been engaged in money laundering, an external report is made the designated official without being subject to the consent or approval of any other person.

As part of the review, other connected accounts or relationships may need to be examined. Connectivity can arise through commercial connectivity, e.g. linked accounts, introducers, solicitors or intermediary etc., or through individuals, e.g. third parties, controllers, signatories etc. However, any need to search for information concerning connected accounts or relationships should not delay the making of a report to NCA.

If, after completing this review, MLRO/ DMLRO/ NO decides that there are grounds for knowledge, suspicion or reasonable grounds to suspect money laundering, then he must disclose the information to NCA as soon as practicable after the disclosure was received in order to avoid committing an offence of failure to disclose.

Nevertheless, care should be taken to guard against a report being submitted as a matter of routine to NCA without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

The MLRO/ DMLRO/ NO will be expected to act honestly and reasonably and to make his determination in good faith. Providing the MLRO/ DMLRO/ NO does act in good faith in deciding not to pass on any suspicions report, and in the absence of knowledge, suspicion or reasonable grounds to suspect money laundering, there should usually be no liability for non-reporting if the judgement is later found to be wrong. However, the decision whether or not to report must not be subject to the consent or approval of any person other than the MLRO/ DMLRO/ NO.

# Awareness and Training

## Training

The Group provide relevant members with necessary training in the key aspects of AML requirements, as set out in this manual.

The Regulations require all firms to take reasonable care to provide appropriate anti-money laundering training for staff that handle, or who are managerially responsible for handling, transactions which may involve money laundering.

The Proceeds of Crime Act 2002 provides that the absence of adequate training by an employer, as required by the Regulations, will provide a defence for staff against a criminal charge of not reporting knowledge or suspicion of money laundering. The defence, however, is not available where a member of staff would have had reasonable grounds to suspect that money laundering was taking place.

## Contents and Methodology of Training

In taking reasonable care, the Group will provide all relevant staff ‘awareness training’ which:

1. deals with the law on money laundering and the responsibilities of staff under the firm’s arrangements;
2. is applicable to all staff who handle or are managerially responsible for the handling of transactions which may involve money laundering; and
3. takes place with sufficient frequency to ensure that within any period of 24 months it is given to substantially all of the staff referred to in (b).

## Approach, Timing and Periodicity of Training

Whilst there is no standard way to conduct staff training for money laundering purposes, the vital requirement is that staff training must be relevant to those being trained and the training

messages should reflect good industry practice.

Induction training in money laundering prevention, recognition and reporting of suspicions, and the CDD requirement will be given to relevant staff at the start of their employment in that role. Relevant staff are those who handle or are managerially responsible for dealing with the applicants for loans (credit broking) or handling transactions and/ or relationships with the students.

The frequency of training for relevant staff is determined on a risk based approach and we believe that, considering the nature of the Group’s business, a refresher training for AML awareness should be provided to all relevant staff at least once in two years. Any new relevant member of staff will also be given this training as early as possible and, in any case, before they begin to deal with loan applications.

The requirement for training to be given within any period of 24 months does not preclude a rolling programme of training, under which training for different employees on different subjects takes place on different dates.

The Group will employ a combination of a) staff sign-off to seek their confirmation that they have read and understood the requirements and obligations under this AML policy and b) computer-based training programme.

# Record Keeping

The Regulations require firms to take reasonable care to make and keep adequate records (including customer identification and accounting records) which are appropriate to the scale, nature and complexity of its business. The Group’s record keeping requirements are set out below.

## Documents verifying evidence of identity

In relation to the evidence of a customer's identity, the Group must make and keep the following records:

1. a copy of the identification evidence obtained; or
2. a record of where a copy of the evidence of identity can be obtained.

Records of identification evidence must be kept for a period of at least five years after the relationship with the customer has ended. The date when the relationship with the customer

has ended is the date of:

* + the carrying out of a one-off transaction or the last in the series of transactions; or
  + the ending of the business relationship, i.e. the closing of the account or accounts.

Where formalities to end a business relationship have not been undertaken, but a period of five years has elapsed since the date when the last transaction was carried out, then the five year retention period commences on the date of the completion of the last transaction.

Where the Group has reasonable grounds for believing that its customer has become insolvent, and it has taken steps to recover all or part of a debt owed by the customer, a record of the steps taken must be retained for five years from the date of the insolvency.

## Transaction records

The OU will retain, for at least five years, records of every introduction made to its affiliate for a loan or any other transaction undertaken for a student in respect of relevant financial business or regulated activity. The precise nature of the records required is not specified, but the objective is to ensure, in so far as is practicable, that in any subsequent investigation the Group can provide the authorities with the relevant documentation and audit trail.

## Internal and External Reports

The Group will also retain:

* + records of action taken under the internal and external reporting requirements; and
  + when an MLRO/ DMLRO/ NO has considered information or other matter concerning knowledge or suspicion that another person has engaged in money laundering, but has not made a report to NCA, a record of that information or other matter.

Records of all reports should be retained for at least five years. Records of reports that are known to be assisting with investigations should be retained until the Group is advised by the investigating officer that they are no longer needed. If the Group has not been advised that an investigation is underway five years after the report was made, then subject to a decision to be made by MLRO/ NO, records need not be retained for a longer period.

## Awareness and Training

These records must be kept for a minimum of 3 years from the date of an employee leaving the role for which they were trained or date of leaving the employment and should include:

* + dates when anti-money laundering training was given;
  + the nature of the training; and
  + the names of the staff who received the training.

# Consequences of Breach

## Consequences for the Group

If investigation of a fraud or money laundering operation revealed that the Group and/ or an employee has carried out or has been associated with any part of a money laundering activity or process, the reputation of the Group will be adversely affected.

Directors/ senior managers of the Group can be fined or imprisoned.

## Consequences for Employees

Every member of staff is required to report to the MLRO/ DMLRO/ NO by completing a Money Laundering Report if he/she knows, suspects, or has reasonable grounds to suspect that an activity or transaction involves Fraud or Money Laundering.

Failure to complete this form in such cases could result in Disciplinary Action and even result in criminal prosecution.

## Criminal Prosecution

The law imposes personal obligations**.** These personal obligations apply to all staff of the relevant financial services firms. Members of staff are protected against criminal prosecution by reporting their suspicion to the MLRO/ DMLRO/ NO.

A timely report of suspicion is a defence in law against a charge of assisting a money launderer.

By reporting a suspicion of money laundering, members of staff are also protected by law against being sued by the customer for breach of confidentiality whether prosecution follows or not.

## Appendix I

**RISK ASSESSMENT MATRIX**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Type** | **Inherent Rating the pr type)** *Lo Medium*  *High (3)* | **Risk (for duct-** *w (1),*  *(2) or* | **Mitigation/ Controls** | **Residual (Post- Control) Risk Rating** |
| **Product & Service**  1. Ability to transfer or assign funds by customers | Low (1) | | * Loan amount is paid directly to the OU by OUSBA. Transfer or assignment of funds by customers is not possible or permitted | Low (1) |
| 2. Private banking service | Low (1) | | * No private banking service if provided | Low (1) |
| 3. Cash payments and receipts | Low (1) | | * Loan is paid to the course provider (OU) (no upfront ‘source of funds’ risk) * No cash payments are accepted from customers | Low (1) |
| 4. Making payments | High (3) | | * Payments from third parties, if they are not related to the   students, are accepted after due diligence (KYC checks)   * There is a residual risk that such checks are not carried out due to insufficient information provided by the student/ third party | Medium (2) |
| to or accepting |  | |  |
| payments from third |  | |  |
| parties |  | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Party (customer)** |  | * Customer on-   boarding checks carried out  electronically include PEPs/ Sanctions   * Checks for non-UK students are not done electronically and a manual check against HMT’s Sanction list will be conducted. We believe that there is no PEP risk associated with our student loan product |  |
|  |  | Low (1) |
| 5. Customers falling | Medium (2) |  |
| in to ‘high risk’ |  |  |
| category, such as |  |  |
| PEP or ‘sanctioned’ |  |  |
| individual |  |  |
| 6. Customers with a fraudulent/ criminal history | Medium (2) | * Fraud alerts and other risk flags checked as part of AML verification electronically | Low (1) |
| **Jurisdiction** | High (3) | * No customers are accepted from the ‘high-risk’ countries or jurisdictions as published by FATF and notified by HMT. Only customers   resident in the  UK/EEA countries are eligible for our loan products. | Low (1) |
| 7. Customer |  |  |
| resident in a |  |  |
| jurisdiction |  |  |
| categorised as ‘high |  |  |
| risk’ by FATF/ HMT |  |  |
| 8.Non-UK  customers | Medium (2) | * Non-UK customers currently accepted are from EEA countries which are either members of the EU or follow equivalent standards such as Norway, Liechtenstein, Monaco and San Marino | Low (1) |

|  |  |  |  |
| --- | --- | --- | --- |
| **Distribution** |  | * The risk is mitigated by following a level of standard due diligence through a credit check (for UK students) with the additional mitigation provided by the fact that the loan is paid directly to the course provider (the OU). However, currently the Group is unable to conduct a credit check on non-UK students, which represents a small residual risk (as such students form a small part of the overall loan portfolio. Manual checks are required to be undertaken for them to mitigate the risk. |  |
|  |  | Medium (2) |
| 9. Non face to face | Medium (2) |  |
| customer |  |  |
| relationship (from |  |  |
| the Group’s |  |  |
| perspective) |  |  |
| 10. Introductions from unregulated firms/ third parties | Medium (2) | * Customers sourced via non-regulated FCA regulated firms/ marketing agents are subjected to the same standard due diligence by the Group as for any direct customers | Low (1) |

### Overall risk rating Medium (1.9) Low (1.2)

**Appendix 2**

**CLIENT IDENTIFICATION/ CUSTOMER DUE DILIGENCE**

**ESTABLISHING IDENTITY - PRIVATE INDIVIDUALS**

The following information should be established and independently verified: True full name and/ or names used;

current permanent address, including postcode.

The source of funds i.e., how the payment was made, from where and by whom, should also be recorded.

### UK Resident Private Individuals

The following is a list of suitable documentary evidence for UK resident private individuals. To guard against forged or counterfeit documents, care should be taken to ensure that any documents offered are originals. Copies may be taken and certified as “Original Seen”.

**List A - *Personal Identity Documents*** (Any one piece required) Current signed passport.

EEA member state Identity Card.

Current EEA or UK Photo-Card Driving Licence.

Current full UK Driving Licence (old version) - old style provisional driving licences should not be accepted.

Valid HM Forces identity Card that includes photograph

(Alternatively, this can be done electronically by conducting a satisfactory credit search)

**List B - *Documentary Evidence of Address*** (Any one required, in addition to the above)

Utility bill or certificate (within last six months) (Care should be taken to guard against accepting mobile telephone bills that can be sent to different addresses).

Local authority tax bill (valid for the current year).

Bank Statement (within last six months) with named person at the correct address

Current UK driving licence (old full licence or new photo-card licence) if not used for evidence of name. (Old style provisional driving licences should not be accepted).

EEA member state Identity Card.

(Alternatively, this can be carried out electronically by conducting a Voters Roll check)

### Non UK Resident Private Individuals

For those prospective customers who are not normally resident in the UK but who make face to face contact, passports should generally be available as evidence of the name of the customer. The national identity cards issued by most EEA countries provide a credible evidence of both name and address and as such a copy of this document should suffice for verifying customers’ identity. Copies of the pages containing the relevant information should be taken e.g., the pages containing the relevant reference numbers, date, and country of issue, or the relevant information should be recorded in the customer’s records as part of the identification evidence.

A document confirming their name and permanent residence (such as a valid Driving Licence or recent

Utility Bill/ Bank Statement) should be obtained where the national identity cards containing the name, date of birth and address are not available.

### ESTABLISHING IDENTITY – UNINCORPORATED BUSINESSES/ PARTNERSHIPS

Where the applicant is an unincorporated business or a partnership whose principal partners/controllers do not already have a business relationship with the Group, identification evidence should be obtained for the partners/ principal beneficial owners / controllers on the same lines as for private individuals. Additionally, the following documents should be obtained, as applicable:

* Partnership Deed and/or Mandate from the Partnership in favour of a partner to enter into transaction on its behalf.
* Evidence of trading/business address.
* Copy of latest report/accounts, if applicable.

### ESTABLISHING IDENTITY - CORPORATE CUSTOMERS

The identity of a corporate company comprises:-

* + its registered number;
  + its registered corporate name and any trading names used;
  + its registered address and any separate principal trading addresses;
  + its directors;
  + its owners and shareholders; and
  + the nature of the company’s business.

Accordingly, the following evidence should be obtained for all companies with whom business is to be transacted:

1. Copy of the latest available report and accounts
2. A Companies House Search (an electronic search may be undertaken)
3. Nature of company’s business
4. Articles/Memorandum of Association

Additionally, the Group should conduct the individual identification procedures as described above in order to verify the true identity and address of the following persons:-

1. Directors
2. Owners
3. Shareholders owning >25 per cent of share capital
4. Principal beneficial owners /controllers
5. signatories to the account

## Appendix 3

### MONEY LAUNDERING SUSPICION REPORTING FORM

**TO: MONEY LAUNDERING REPORTING OFFICER/ DMLRO FROM**:

Name: ………………………………………………………………….. Tel: …………………………………

Position/ Job Title: …………………………………………………

**CUSTOMER/CLIENT:**

Name(s): …………………………………………………………………………………………….……………

Permanent Address: ………………………………………………………………………………………..…..

…………………………………………………………………… Date of Birth: ………………………………

Nationality/Country of Residence: ……………………………………………………………………….…….

Business/Occupation/Profession/Employer: …………………………………………………………………

Account No/Customer Ref: …………………………………………………………………………………….

Date Relationship Commenced: …………………………………………………………..

Normal Account Activity: ………………………………………………………………………………………. (size and nature of transactions)

……………………………………………………………………………………………………………………… Connected Accounts: ……………………………………………………………………………………………



………………………………………………………………………………………………………………………

**INFORMATION/SUSPICION:**

Transaction/Instruction: …………………………………………………………………………………………

Reason for suspicion: …………………………………………………………………………………………... (please attach copies of relevant documents)

………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………

Reporter’s Signature………………………………………… Date: ………………………………………….

*Note: It is a criminal offence to advise the customer/client or anyone else of your suspicion of that a suspicion report has been made.*

For MLRO/ DMLRO’s use:

Date received: ………………….. Time received: …………………….. Ref:

…………………………

NCA advised?: Yes/No

Date: ………………………………… Ref: …………………………

NCA consent required: Yes/No Date consent request submitted:

obtained/withheld