PROCUREMENT

POLICY

Policy no:	9.5
Version no. & date:	V23.4
Next review due:	September 2024
Responsible Committee:	SMT
Approved by & date:	May 23
Linked policies:	Other GDPR Policies
External references	GDPR, Data Protection Act 2018

Audience:	Internal

Contents

1 Introduction

At the heart of this policy is our commitment to achieving the best value for money, enhancing efficiency and effectiveness, and promoting fair competition, while maintaining the highest level of integrity, standards of accountability, and the prudent use of public and institutional resources.

This Procurement Policy helps us meet our strategic objectives and operational needs in accordance with applicable laws and regulations, and it supports our principles of sustainable and responsible procurement. As such, this policy should be read and understood by all those involved in the procurement process within our organization. This procedure additionally outlines how suppliers to Oxford Business College (The College) who process personal data on behalf of the College (Processors/Sub Processors) or have access to College systems, should be assessed to ensure they have appropriate levels of security in place and comply with the GDPR.

2 Purpose

The purpose of this Procurement Policy is to guide the acquisition of goods, services, and works at our institution, ensuring that all procurement activities are conducted in a fair, transparent, and ethical manner. This policy establishes the principles and procedures that our employees, contractors, and partners should follow when procuring goods or services on behalf of the organisation.

3 Scope

The scope of this procedure covers all suppliers to the College who either process personal data on behalf of Oxford Business College (Processors/Sub Processors) or have access to College systems.

4 Responsibilities

All staff are responsible for ensuring that, prior to onboarding a new supplier who processes personal data on behalf of Oxford Business College (Processors/Sub Processors), or has access to College systems, this process is followed.

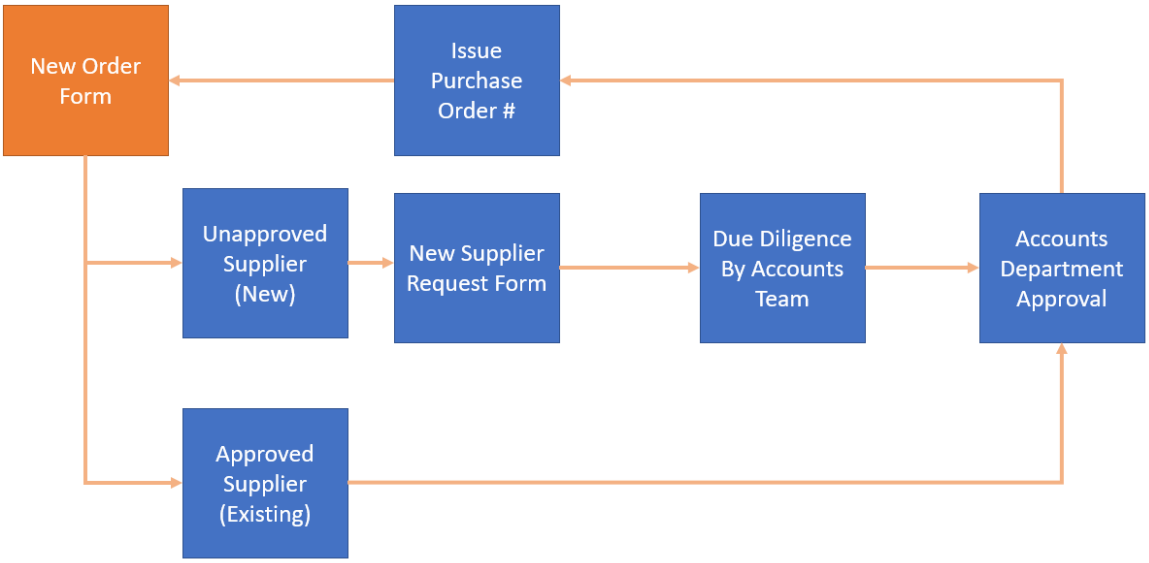
The employee who instigates a request for a new supplier is responsible for updating the supplier due diligence record.

The Accounts department is responsible for reviewing the supplier due diligence questionnaire answers from the supplier and making a recommendation on whether the supplier can be used.

The Head of Operations & DPO is responsible for reviewing the supplier due diligence record monthly and arranging annual due diligence reviews of existing suppliers.

The Managing Director is responsible for making the final decision as to whether the supplier will be used. This will be done at sign off.

5 Procedure



When a "**New Order**" is required, an New Order Form must be completed.

- If the Supplier of this order is Unapproved (NEW):
    - A "New Supplier Request Form" must be completed
    - Accounts will need to complete "Due Diligence" based on protocols pre-established.
    - Once the Supplier is approved The Accounts team then approves the order.
    - Approval of the order is established by the Accounts Team issuing a Purchasing Order.
- If the Supplier is an Approved Supplier (Existing):
    - Accounts department will be required to approve the order#
    - Approval of the order is established by the Accounts Team issuing a Purchasing Order.

Accounts Department Approval:

Approval process of Accounts Department:

a) The supplier will be processing personal data on behalf of the College

b) The supplier has access to College systems which may give access to personal data

If the answer is no, no further action is needed in relation to this procedure. If the answer is yes to

either of the above, the following process should be followed:

- The **Supplier Due Diligence Questionnaire** should be sent to the key contact at the supplier asking them to complete it and return within a given timescale. It should be explained to the supplier that this is part of Oxford Business College supplier due diligence process.

- Once the completed questionnaire is received, this should be passed to the Accounts Department for review along with contact details of the supplier. If there is Data being transferred that belongs to Oxford Business College the DPO should also be informed and the GDPR due diligence check should be completed [Appendix 2].

- The Accounts Department & if required the DPO will review the questionnaire and raise any questions they may have with the supplier directly. They may ask at this point if the supplier is able to address any issues and apply additional controls in order to satisfy their requirements.

- The Accounts Department will decide as to the suitability of the supplier in the form of a recommendation which would either be to go ahead with the supplier or do not use the supplier.

- The Accounts Department decision will be provided to the Managing Director as part of the supplier sign off process.

- The Managing Director will make the final decision as to whether the supplier can be used and notify the Accounts Department of this.

- The Accounts Department will issue a Purchasing Order which will be sent to the individual or department making the order.

- The employee who instigated the new supplier will complete the supplier due diligence record to record the new supplier.

- The Accounts will review the supplier due diligence record monthly.

6 Reviewing Due Diligence

Supplier due diligence should be conducted on an annual basis to ensure the supplier is maintaining their security and GDPR compliance.

Appendix:1

New Order Form: https://forms.office.com/e/egaRXWeKra

Supplier Due Diligence Questionnaire: https://forms.office.com/e/WiAtCLXReE

Appendix 2 – GDPR Due Diligence check

Supplier Due Diligence Questionnaire

Company Details

No	Company Details	Answer
1	Company Name	
2	Company Registration No	
3	Country registered in	
4	Company Address	
5	Location of where processing activities are taking place	
6	Name of main point of contact	
7	Main point of contact email address	
8	Main point of contact phone number	
9	Services provided	

GDPR

No	GDPR Requirements	Answer (Y/N)	More Detail/Comments
1	Do you have a DPO (if yes, please provide contact details in answer)	Insert names of any documents provided as evidence	Provide further details as requested in the question
2	If you do not have a DPO, please provide contact details of the nominated individual in your organisation with data protection responsibilities		

3	Do you have up to date records of processing in accordance with Article 30		
4	Do you have an internal Data Privacy Policy? If yes, please provide evidence		
5	Do you have a data subject rights request procedure ? If yes, please provide evidence		
6	Do you have a data retention policy or procedure? If yes, please provide evidence		
7	What is the process of disposing of personal data and hardware?		
8	Do you train your staff on their data protection responsibilities? If so, please detail how often and what is covered		
9	Do you have a Data processing agreement for processing our data? If so, please provide a copy		
10	Are signed contracts in place (complete with confidentiality clauses) for all staff/contractors and volunteers?		
11	Do you have up-to-date privacy notices for customers/clients and for employees?		
12	Do you use tracking pixels on your website or in any emails you send?		
13	Do you have a formal method of risk assess processing carried out on personal data e.g. DPIAs and a risk framework?		

Third Parties

No	Sub processors/sub contractors and third parties	Answer (Y/N/NA)	More Detail/Comments

1	Are any third parties or contractors involved in the data processing activities you perform for us? If so, please provide details including names and what function they perform	Insert names of any documents provided as evidence	Provide further details as requested in the question
2	If third parties or contractors are used, are they trained on their data protection responsibilities? Please provide details of how often and what is covered		
3	Please provide details of how you assess the security measures used by any third parties and their compliance with GDPR - please provide any due diligence questionnaires or assessments you use		
4	If you transfer to third parties, are these third parties accessing our personal data from outside the EEA or from a country that does not have an adequacy decision? If yes, please provide the details of the countries and details of safeguards you have implemented to address this		
5	Do you have data processing agreements in place with any third parties handling our personal data? If yes, please provide copies.		

Data Breaches

No	Data Breaches	Answer (Y/N)	More Detail/Comments
1	Do you have a data breach policy & procedure in place? If yes, please provide a copy	Insert names of any documents provided as evidence	Provide further details as requested in the question
2	Do you have a data breach log?		
3	Have you had any data breaches in the last 12 months? If yes, please provide details of breach, remediation actions, whether it was reportable and what, if any,		

	fines/enforcement actions were applied

Information Security

No	Security	Answer (Y/N)	More Detail/Comments
1	Are you certified to any particular information security standard e.g. Cyber Essentials, ISO 27001? If so, please provide certificates	Insert names of any documents provided as evidence	Provide further details as requested in the question
2	Do you have an information security manager/CISO or other person responsible for information security? If yes, please provide contact details		
3	Do you have an information security policy? If so, please provide a copy		
4	Do you encrypt the personal data you process for us at rest? If yes, please provide details		
5	Do you encrypt the personal data you process for us in transit? If yes, please provide details		
6	Have you implemented anti malware on all devices involved with the processing of personal data		
7	Have you implemented a patching strategy formulated in line with good practice for software and firmware? If yes, please provide details		
8	Within your organisation do you employ role based access control measures		
9	Do you allow remote access or mobile working that could		

	access the personal data you process for us? If yes, what security measures are in place for this?	
10	Do you implement pre employment screening, take references prior to employment?	
11	Do you operate a clean desk/clear screen policy? If yes, please provide details	
12	Do you have annual penetration tests? If so, please provide details of your last test	
13	Do you conduct regular vulnerability scanning? If so, please provide details of your last scan	
14	Do you provide software applications/solutions to us that you develop in house or you control, if yes, please provide details of secure software development best practices followed	
15	Do you have a risk management framework to assess information security and privacy risks in your business? If yes, please provide details	
16	Do you have a business continuity plan? If so, has this been tested and when?	
17	Do you apply server and network protection including the use of firewalls and other network based devices e.g. IDS/IPS? If yes, please provide details	

Review (to be completed by the DPO)

Assessment reviewed by	
Job Role	

Date Reviewed (dd/mm/yyyy)	
Outcome	
Additional information requested (if outcome is more info needed)	
Date additional information requested (dd/mm/yyyy)	
Additional information provided	
Final decision	
Date of final decision (dd/mm/yyyy)	
Date of next review (dd/mm/yyyy)	