RICHMOND, THE AMERICAN INTERNATIONAL UNIVERSITY IN LONDON, INC.

Third Party Policy

Version 1.1 – April 2023

_____

Purpose

The purpose of this document is to define the policy for selecting third party suppliers for Richmond University. It should be read alongside the overall Procurement Policy, held by Finance

Scope

The policy covers all third-party selection for services at Richmond University.

Policy

When a supplier is selected contracts/agreements/terms and conditions are to be raised and passed to the Finance team and the Data Protection Officer for due diligence review.

In circumstances where a supplier is unable to meet all requirements of applicable data privacy legislation, the decision to engage them must be made by the University Board on balance of risk and that risk recorded via the IT and Data Governance Group (ITDGC).

Confidential or personal data should not be exchanged with a third party in advance of a formal agreement being in place.

Confidentiality

Before any Richmond University data (that is not classified as Public) is transferred or accessed by a third party there must be a suitable contract or disclosure agreement to cover the confidentiality of the data in scope of the service. As a minimum this must cover:

- Type of data
- Length of agreement
- Data usage scope
- Non-disclosure

Procurement

The procurement of new or renewing services with third parties must not be concluded without going through the data privacy impact assessment (DPIA) process and the Finance department's new supplier processes (including but not limited to IR35 and fraud control compliance). To start the DPIA process, email the Data Protection Officer to assist in completion of the DPIA as soon as possible to avoid delay to the review.

When considering a third party for the provision of service the following should be used as a guideline to reduce the risk involved with using this third party:

- The reputation of this third party
- The location of the third party and their service (when the data is classified as personal data this must be in the UK, the European Economic Area or an adequate country. Alternatively, there must be an appropriate and EU Commission recognised safeguard in place, this may be revised as the UK works through its Brexit plans with regard to data privacy legislation)
- The standards the third party measure themselves by, such as:
    - ISO 27001
    - ISO 27018
    - ISO 9001
    - PCI DSS
    - SOC II
    - Cyber Essentials

The IT DGC will take responsibility for the review of the third party and the information security stance they adopt. This will include:

- Review of the service definition.
- Review of the Richmond University data in scope for this service.
- Assessment of any risks associated with the third party and the service.
- Where risk is identified, the risk will be treated and recorded.
- If the risk of service implementation is identified to be medium or high after the risk review, it will be taken to the SLT for further mitigation / decision.
- Where the risk includes personal data (as defined in the Data Protection Act 2018), a full Data Privacy Impact Assessment will be completed
- Where the risk includes personal data (as defined in the Data Protection Act 2018), the DPO will request the third party to complete the Richmond University Third Party Supplier Questionnaire to further assess their security risk.

Third Party Contracts

The below is in addition to the section on Confidentiality in this policy.

Where a third party requires access to and the processing of personal data (as defined in the UK Data Protection Act 2018) on behalf of Richmond University, a contract/agreement structure will need to be in place that aligns to the following criteria:

Compulsory contract clauses:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

The following are also clauses that should be included in all contracts with third parties who process personal data:

- the third party must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the third party must ensure that people processing the data are subject to a duty of confidence;
- the third party must take appropriate measures to ensure the security of processing;
- the third party must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the third party must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the Data Protection Act 2018;
- the third party must assist the data controller in meeting its Data Protection Act 2018 obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the third party must delete or return all personal data to the controller as requested at the end of the contract; and
- the third party must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the Data Protection Act 2018.

Third Party Reviews

All third parties will be reviewed in accordance with this policy and against the following schedule:

- Contract renewal
- Service change
- Annually where the contract has no term

Revision History

Version	Change	Author	Date of Change
1.0	Initial version	Paul Saunders	28-01-22
1.1	Minor clarifications on procurement process and template change	Paul Saunders	05-04-23