1 Introduction

There are some functions across LSE that can require credit card payments. LSE is obliged to meet the Payment Card Industry's Data Security Standard (PCI DSS), and has a policy stating its commitment to maintaining compliance – the PCI DSS Compliance Policy. The policy outlines the ways in which LSE can use or build systems that process credit card payments, and how the card payments must be handled.

In essence, to achieve PCI DSS compliance LSE *must* outsource card processing to a compliant third party. The focus of LSE's information Management and Technology Division must be directed towards underpinning teaching and research, not providing security and assurance around payment activities.

As LSE is required to monitor the compliance status of its credit card service suppliers annually, it must avoid an overly complex situation where services are provided by a heterogeneous range of suppliers, and concentrate card services as much as possible. This approach dovetails with the Finance Division's project F0141180 "Online Card Payment Platform", which this policy is intended to support.

1.1 Scope

All new functions/services containing a card payment element, unless robust business reasons exist why a separate and dedicated card payment gateway must be used (for instance, in the case of Residences' Property Management System or catering System).

1.2 Out of Scope

Existing externally-hosted card gateways that are PCI DSS compliant.

2 Policy

2.1 Principles

All payment gateways used must be externally hosted and must themselves demonstrate active and ongoing PCI DSS compliance.

If a function/service does not already have a PCI DSS compliant method of taking credit card payments, *all* its online credit/debit card transactions will be performed via a pre-existing e-shop service, currently provided by WPM. All future services, if they do not have a valid business justification for a separate payment gateway, will be have credit and debit card payments processed by LSE's pre-existing e-shop function.

This approach supports the continual improvement plan incorporated into project F0141180 "online card payment platform."

This solution will not be retrofitted to existing PCI DSS compliant payment solutions. There will however be an ongoing review of existing services by the Finance Division as part of F0141180.

All exceptions will require a project mandate/business case approved by PRB/ITPB. There will be no ad hoc exceptions.

2.2 Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath LSE's overarching *Information Security Policy*. Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE's website. All staff, students and any third parties authorised to access LSE's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

A full list of existing information security policies can be found at:
http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/home.aspx.

2.3 Review and Development

This policy shall be reviewed and updated regularly by the Information Security Advisory Board (ISAB) and an auditor external to IMT if required to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.

3 Responsibilities

Function/Service Owners
Function and service owners are responsible for becoming PCI DSS compliant and remaining PCI DSS compliant.

Finance Division
Responsible for:

- Project F0141180 “Online Card Payment Platform”
- LSE’s relationship with its acquirers
- Settlement

PCI DSS Compliance Group
Responsible for:

- Liaising with LSE’s acquirer around PCI DSS compliance
- Submitting PCI DSS Self-Assessment Questionnaires annually
- Reporting any non-compliance
    - To the COO and CFO
    - To the School’s acquirer
- Advising function and service owners on required compliance activities
- Conducting annual audits of compliance
- Provision of PCI DSS training

Information Security Manager:
Responsible for writing this policy and establishing access control principles.

Information Security Team
Responsible for:

- assessing Cloud Questionnaire responses, with signoff on whether cloud systems can be used
- investigating breaches and recommending remedial actions
- organising annual penetration tests

Information Security Advisory Board
Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee
Responsible for approving information security policies.

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy Information Classification Standard	3.7 3.0	01/07/15 15/03/13	Jethro Perkins Jethro Perkins

Version history

Date	Version	Comments
07/10/16	0.1	Initial version
09/12/16	1.0	Approved by Information Technology Committee 05/12/16. Moved to release.

Review control

Reviewer	Section	Comments	Actions agreed