2 Responsibilities

Divisions / Departments / Projects
It is the responsibility of any division, department or project that is implementing a solution requiring the storage, transmission or processing of cardholder data to ensure that this solution is PCI DSS compliant, and meets with the achievable levels of PCI DSS compliance laid out in *Section 3.2* of this policy.

PCI DSS Compliance Group
- Ensuring ongoing assessment of payment streams that have achieved PCI DSS compliance under the PCI DSS project.
- Compliance guidance for any future projects.
- Assessment of capability to meet Self-Assessment Questionnaire levels.
- Control of Security Awareness Programme.
- Assessing and reviewing PCI DSS-specific information security policies.
- Maintaining at least two PCI-qualified Internal Security Assessors within the School
- Stating what SAQ categories of compliance are feasible within the School

PCI DSS Project
- Ensuring PCI DSS compliance of existing identified payment streams is achieved

IMT PMO
- Ensuring awareness of potential PCI DSS compliance is brought to the attention of the Compliance Group at Project Mandate and Business Case stage
- Referring any projects (existing or potential) that require credit or debit card payments to the Compliance Group that have otherwise not been previously identified as requiring PCI DSS compliance

Information Security Manager:
- Reviewing all Project Mandates and Business cases that pass through PMO
- Chairing PCI DSS compliance group
- Administering Security Awareness Programme
- Developing, maintaining and reviewing appropriate PCI DSS-focused Information Security Policies
- Authorising blocks on any non-compliant payment stream that has not been explicitly authorised for operating by the Director of Finance or the Chief Financial Officer
- Assessing the School's posture against SAQ requirements and recommending to the Compliance Group where compliance is possible

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.

Director of Finance / Chief Financial Officer
Responsible for the explicit written sign-off for any non-compliant payment stream or non-compliant element of a payment stream in order for its operation to continue.

Responsible for signing off the Self Assesment Questionnaires for each payment stream.

School Secretary
Required, along with one of Director of Finance/Chief Financial Officer, to provide explicit sign off for any non-compliant payment stream or non-compliant element of a payment stream in order for its operation to continue

3 Policy

3.1 Compliance overview

LSE is currently defined by its acquirer as a **Level 3** merchant, meaning it processes between **20,000** and **1,000,000** transactions per card brand per year.

As a result of this, LSE is required to fill in Self-Assessment Questionnaires (SAQ) annually to demonstrate its level of compliance with the PCI DSS standard. Different Self-Assessment Questionnaires are required for different payment categories, as laid out below. Different categories require compliance with different controls from the complete PCI DSS control set. Compliance with all controls is only required by PCI DSS SAQ D category payment card streams.

3.2 Achievable PCI DSS levels of compliance for LSE

LSE can achieve compliance at PCI DSS version 3 for the following categories:

SAQ A : "applicable to merchants whose cardholder data functions are completely outsourced to validated third parties" and where "The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s)"

SAQ B : "applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals" and where "The standalone, dial-out terminals are not connected to any other systems within your environment"

SAQ P2PE-HW "applicable to merchants who process cardholder data only via hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption (P2PE) solution"

Caveat

Achieving these levels requires careful planning and implementation, including enrolment of staff in a PCI DSS security awareness programme.

Compliance for any application or project is not achieved ***by default*** of other projects being compliant, and *always* requires a project and interaction with the PCI DSS Compliance Group.

3.3 Unachievable levels of PCI DSS compliance

With the current levels of resource in IMT, the networking technologies curently in place, and a primary focus for those resources on supporting teaching and research activities, the following types of compliance are not achievable

SAQ A-EP : "e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data". Applicable where the cardholder data is entered into a merchant's website and then forwarded on to a PCI DSS compliant third party for processing.

SAQ B-IP : "applicable to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction (POI) devices with an IP connection to the payment processor" and where "The standalone IP-connected POI devices are not connected to any other systems within your environment (this can be achieved via network segmentation to isolate POI devices from other systems)"

SAQ C : "applicable to merchants whose payment application systems (for example, point-of-sale systems) are connected to the Internet (for example, via DSL, cable modem, etc.)"

SAQ D : "applies to SAQ-eligible merchants not meeting the criteria for any other SAQ type"

3.4 Levels of PCI DSS under assessment

SAQ CVT : " merchants who process cardholder data only via isolated virtual payment terminals on a personal computer connected to the Internet". This is required by Advancement.

3.5 Options for any project requiring unachievable levels of PCI DSS compliance

1. Outsource processing, storage and transmission of credit card data to a PCI DSS compliant company in such a way that LSE compliance can be achieved under levels defined in 3.2.
2. Change the scope of the project so that LSE compliance can be achieved under levels defined in 3.2.
3. Provide resources for ongoing compliance at levels defined in 3.3. This would require major a re-orientation of School-wide resources
4. Gain explicit sign-off from the Director of Finance or the Chief Financial Officer in order to accept the risks (including LSE receiving unlimited fines and/or the removal of its ability to process credit and debit card payments) of non-compliance

3.6 Non-compliance

There may be circumstances where one element in the chain of compliance required by the PCI DSS standard cannot be achieved. For instance, while a room booking system may be hosted in a PCI-DSS compliant environment, with the on-site components also successfully assessed against the appropriate SAQ, the Online Travel Agent (OTA) used as a payment channel may not be compliant, and may have no inducement to become compliant. In this case, the risk of using the OTA must be accepted by the School Secretary and one of either Director of Finance or the CFO, otherwise the payment channel must not be used.

Any instance where non-compliant payment streams are being used within LSE or by LSE tenants in such a manner as to bring LSE within the scope of their compliance requirements, the payment stream will be blocked by IMT from operating. This includes in cases where compliance is theoretically possible (i.e. cases that would fall into categories of compliance defined in 3.2) but where interaction and assessment have not taken place either by the PCI DSS Compliance Group or the PCI DSS project.

3.7 Tenants

As laid out in the 'IMT Support for LSE Tenants' paper endorsed by July 2014 Information Technology Committee, tenants must ensure all credit and debit card payments are processed using leased lines, and are not passed across LSE's network.

3.8 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.

The below list of current policies is in no way authoritative and new policies will be published on the LSE website as they become available.

Associated polices:

Information Security Policy
Conditions of Use of IT Facilities at LSE

3.9 Review and Development

This policy shall be reviewed and updated regularly by the Information Security Advisory Board (ISAB) and an auditor external to IT Services as appropriate 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.