Card Payments Security Policy

Policy Category:	Finance
Subject:	Securing card payment processing
Approving Authority:	SMT
Responsible Officer:	Vice-President (Finance)
Responsible Office:	Finance
Related Procedures:	Card Payments Security Procedures
Related College Policies:	
Effective Date:	November 2020
Supersedes:	N/A
Next Review:	November 2023
Last Review Date:	2nd December 2022

I. Purpose & Scope

The purpose of this policy is to ensure that card payment transactions are processed in a secure manner that is compliant with the Payment Card Industry Data Security Standard (PCI DSS), which is a global industry standard. The College has a contractual obligation with its payment card acquirers to be PCI DSS compliant.

This policy applies to any individual or third party involved with processing, storing, transmitting, or accessing card payment data, where:

- King's is the Merchant or Data Controller
- King's is the Data Processor
- Payment card data is being processed on a King's site

Individuals and third parties include:

- Customer facing staff accepting card payments either face to face, by phone and/or by mail
- Staff maintaining systems connected to or involved with card payments processing
- Payment service providers (PSPs)
- Payment card acquirers

II. Definitions

Customers include students, learners, donors and general customers.
Data Controllers are the individuals who decide on how the card payment data is to be processed, stored and/or transmitted.
Data Processors process, store and/or transmit card payment data.
Merchant is the business supplying the goods or services for sale.
Payment cards are credit and debit cards.
Payment card acquirers are banks or financial institutions that process payment card transactions on behalf of a Merchant and pay the Merchant the funds obtained from credit card transactions.
Payment service providers are third parties who process, store and/or transmit card payment data for the Merchant through to Payment card acquirers. This also includes service providers who host websites which redirect to a secure payment page.

PCI DSS is the Payment Card Industry Data Security Standard which is a global standard written and maintained by the PCI Security Standards Council, whose members include Visa and MasterCard.

III. Policy

1. Risk

1.1 Breach of payment card data will impact King's customers' ability to pay for goods/services with their payment card; may lead to financial sanctions from the UK Information Commissioner and/or payment card acquirers; may result in losing the ability to accept card payments; and may result in significant reputational damage for the College.

2. Secure processing of card payments

2.1 All card payment processing is to be outsourced to a PCI DSS compliant payment service provider. All service providers and/or solutions must be verified and authorised by following the new suppliers setup process prior to any use.

2.2 No payment card data is to be stored on or processed by any King's system or application. This includes and equally applies to your own personal or business purchasing card data.

2.3 No payment card data is to be sent using end-user messaging technologies such as email, instant messaging, SMS and chat systems including MS Teams.

2.4 Documents with payment card details must always be securely stored, transported and disposed of.

2.5 Websites which redirect to a securely hosted payment page must also be formally verified to be PCI DSS compliant. This now includes evidence that the website or web application provider can ensure unauthorised changes on payment redirect pages are detected and responded to via an appropriate change and tamper-detection mechanism.

2.6 Any web page processing card payment data or redirecting to a hosted payment page must use current & correctly implemented encryption techniques and standards as advised by NIST – (National Institute of Standards and Technology.)

3. Implementation and maintenance of card payments processes

3.1 Any new payment card processes must be approved by the Finance, Head of Income Services prior to any contracts being signed.

3.2 Any process to capture card payments details on paper needs to be approved annually by the Finance, Head of Income Services.

3.3 Evidence of the third parties PCI DSS compliance must be validated prior to any processing, storing, or transmitting of payment card transactions. Thereafter the provider/acquirer will be required to annually confirm their PCI DSS compliance with the College.

3.4 Chip and PIN devices must be secured when not in use and have regular, documented physical security checks completed.

4. Governance

4.1 All card processing activities of the College must comply with PCI DSS, the College's Financial Regulations and Procedures and the Data Protection Policy. Roles and responsibilities for performing any activities in relation to PCI DSS or card processing are documented, assigned, and understood.

4.2 A written agreement must be in place with any payment service provider prior to any payment card processing taking place, and the payment service provider must take responsibility for the security of any King's payment card data they process, store, transmit, access, or have the ability to impact.

4.3 Payment card data is personal data as defined in the Data Protection Act 2018 and the data protection clauses need to be included in any payment service provider contract.

4.4 A programme needs to be maintained to monitor payment service providers' annual PCI DSS compliance and to maintain information on the service(s) provided, which PCI DSS requirements are managed by each payment service provider and which are managed by King's.

4.5 King's will suspend any contract with a payment service provider or a payment card acquirer who are no longer PCI DSS compliant.

4.6 A documented risk assessment exercise must be undertaken with specific focus to card payment activity annually or upon any significant changes to the environment.

IV. Enforcement

Following the requirements of this policy, other associated policies and procedures will ensure that users comply with the law. However, users should contact pci-questions@kcl.ac.uk for advice about any concerns.

Non-compliance with this policy or associated procedures is an infringement of King's regulations and will be investigated in accordance with:

- G27 of the Academic Regulations (students)
- College Ordinances and relevant Human Resources Regulations (academic staff)
- College Capability and disciplinary procedures (for staff other than lecturers, senior lecturers, readers and professors).

The CIO or designate, may remove, or limit a user's access to the university's systems on a temporary basis when that is deemed necessary to protect the system or prevent reputational damage to the university or in the course of an investigation.

On the recommendation of the CIO or designate, further access limitations or permanent denial of access may be imposed by the Senior Vice-President (Operations) or designate.

V. Review and Development of this Policy

This policy is reviewed and updated annually.