Card Payments Security Procedures

Effective Date: June 2019
Supersedes: PCI DSS Policy v1.0
Next Review: December 2023
Last Review Date: 2nd December 2022

---

1. Definitions

3D Secure	Added security measure for payments taken online - 3D Secure normally appears to customers as either **Verified by Visa** or **MasterCard SecureCode** and allows the customer to enter additional security details which they themselves have setup with their own card issuer.
Acquiring Bank	Bank that processes card payments for the merchant (King's) and pays the merchant the funds from payment card transactions.
CVV2	Card Verification Value 2 – is the last 3 digits at the back of a payment card, after the card number itself, for Visa and MasterCard cards.
Customer	Includes students, learners, donors and general customers.
DTMF tones	Dual-tone multi frequency tones produced by a phone when pressing the number pad.
Keystroke logger	A device that can record computer keystrokes and/or the details being typed.
Payment Cards	Credit and debit cards.
PCI DSS	Payment Card Industry Data Security Standard - PCI DSS is a worldwide security standard assembled by the Payment Card Industry Security Standards Council www.pcisecuritystandards.org/document_library
PDQ	Process Data Quickly (commonly known as Chip & PIN devices).
PED	PIN Entry Device (commonly known as Chip and PIN devices).
PSP	Payment Service Provider – provides merchants (King's) with the functionality to accept card payments transactions.
SSL Certificate	Secure Sockets Layer Certificate – an electronic certificate that allows secure webpages (beginning with the prefix **https://**) to encrypt the data entered.
PCI Security Standards Council	A global forum responsible for the development, management, education and awareness of the PCI Security Standards. The Council's five founding members are American Express, Discover, JCB, MasterCard and Visa. https://www.pcisecuritystandards.org/about_us/
TLS	Transport Layer Security – is a cryptographic protocol designed to provide communications security over a computer network.
VoIP	Voice over Internet Protocol – is a group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks.

2. Purpose & Scope

2.1 These procedures underpin the Card Payments Security Policy and set out how King's College London will process payment card transactions and how those payment card transactions will be secured, to ensure King's continues to maintain its PCI DSS (Payment Card Industry Data Security Standard) compliance.

2.2 PCI DSS represents a common set of industry tools and measurements to help ensure the safe handling of sensitive payment card information. PCI is a global standard which applies to all

organisations (Merchants and Service Providers) who receive, access, process, store and/or pass on cardholder information. Many of the requirements of PCI DSS are specific to IT Services.

2.3 PCI DSS is designed to protect the cardholder information of customers and any other individual or entity that utilises a payment card to transact business with the College.

2.4 Scope includes any payment card process or access to payment card data and includes systems connected to payment card processing and/or payment card databases.

3. Payment Card Data Compromise

3.1 A data compromise event is an unauthorised and illegal theft or attempted theft of data.

3.2 There are three basic types of data compromise events:

- Physical theft or device manipulation includes stealing documents with card data and replacing existing Chip & PIN card payment devices with manipulated devices.
- Skimming: The thief can copy a card number using basic methods such as photocopying a document with payment card data or more advanced methods such as using a small electronic device (skimmer) to swipe and store a card's magnetic stripe information.
- System Intrusion: Utilising malicious, unauthorised and illegal means to obtain electronic access to payment processing systems, often referred to as hacking.

3.3 In the event of there being a suspected card data compromise or if in any doubt, staff must immediately report it to the IT Service Desk, requesting the ticket to be immediately referred to the Cyber Security team:

Email: 88888@kcl.ac.uk
Phone: 020 7848 8888

4. King's PCI Compliance Strategy

4.1 King's PCI DSS compliance strategy is to outsource all card payments processing and as a result card payment details are to be only processed:

- Face to face: using a secure PCI DSS compliant card payment device that removes the King's network from PCI scope, such as a Chip and PIN device which encrypts the card payment transactions.
- Online: using a secure web payment page hosted by a PCI DSS compliant service provider.
- Over the phone: using secure phone lines, which are managed by a PCI DSS compliant service provider and with the cardholder providing their card details using their phone keypad (solution is called Masked DTMF).

4.2 No processing, storage, transmitting or accessing of payment card data is to be completed using a King's PC / Laptop as King's devices and network are not currently PCI DSS compliant.

4.3 Card payment refunds can be processed via a payment processor portal and does not require the full card number of the originating purchase transaction.

4.4 Only truncated payment card numbers (showing a maximum of the first 6 and the last 4 numbers of the card) or payment card tokens can be stored if absolutely necessary on secured King's SOE (Standard Operating Environment) devices and systems.

4.5 Physical documents that include payment card details can only be stored in King's premises for the following reasons:

- Fundraising campaign letters returned by donors.
- Card details captured on paper from a face-to-face interaction with a cardholder as a result of a Chip and PIN device either not working at the time or unavailable at the time (where this process has been approved by the Finance, Head of Income Services).
- Cardholder dispute / chargeback letters.

4.6 Any paper documents with card payment details need to be tracked and secured in a locked cabinet/safe/drawer prior to being processed, with access limited to authorised individuals only. Once the card payment details have been processed, the paper documents need to be shredded using a cross-cut shredder or as a minimum the part of the document with the card details needs to be removed and shredded.

4.7 Where paper documents with card numbers are being stored (where permission has been provided by Finance, Head of Income Services) it needs to be verified, at least quarterly, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

4.8 Upon request, Finance will initially provide a section with a cross-cut shredder in which to cross-cut shred any written card details received. Subsequent cross-cut shredders will then need to be purchased by the section themselves.

4.9 On completion of a successful payment, a payment confirmation needs to be generated and sent to the customer.

4.10 If card payment details have been received by email, then the email must be deleted from the inbox and also from the deleted mail folder. If the email requires a response, the card information provided must be removed from the email before reply. At no point must an email containing card details ever be saved. The customer must also be advised against sending us their card details in this way again for their own protection.

4.11 Any new payment card channel used by a King's department must follow these principles:

a. As per 10.10.1.3 of the Financial Procedures – where departments require the facility to take card payments other than for the collection of student fees e.g. for transcripts and conference payments, they need to contact the Finance, Head of Income Services prior card processing agreement.
b. All card payment processing needs to be outsourced to a PCI DSS compliant processor.
c. All service providers involved with the card payment processes or with access to the payment card data need to be already PCI DSS compliant and be able to provide a PCI DSS Attestation of Compliance (AoC) prior to any transactions being processed.
d. A proper due diligence of any new payment service provider needs to be completed by both the King's Cyber Security team and the Finance, Head of Income Services.
e. The payment service provider contract must include the following clauses:
    - Data protection clauses which sets out how they will:
        - maintain PCI DSS compliance.
        - use only PCI DSS compliant processors.
        - comply with the UK Data Protection Act 2018.

- Be responsible for any payment card data breach.
- Inform King's of any suspected data compromise immediately.

f. Any new payment card processing contract must be reviewed by both King's Procurement and Legal Counsel prior to being signed.

4.12 An annual (dates within the past 12 months) PCI DSS Attestation of Compliance (AoC) document is required for all third parties involved with payment card processing, proving their continued PCI DSS compliance. These documents need to be sent by email to PCI-confirmations@kcl.ac.uk

5. Online Payments

5.1 Online payment processing is the preferred method and best practice for taking payments.

5.2 Departments must not under any circumstance make their own arrangements with Payment Services Providers. Rather, they must contact Procurement and the Finance, Head of Income Services beforehand and where possible make use of existing / preferred service providers. Please read the KCL New Supplier Setup process for further details about contracting with a new supplier.

5.3 For added customer security, 3D Secure needs to be enabled for online payments taken by King's. 3D Secure normally appears to customers as either Verified by Visa or MasterCard SecureCode and allows the customer to enter additional security details which they themselves have setup with their own card issuer. At no point must a customer ever be asked to divulge their 3D Secure password or card CVV2 / PIN numbers.

5.4 For online payments, card details must always be captured on a payment page which is hosted by a PCI DSS compliant PSP (payment service provider). Other associated requirements:

a. Where the customer is redirected from a web page (originating web page) to a securely hosted payment capture page, as usually is the case, that originating web page must also be hosted by a third party, 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.
   - For King's to maintain PCI DSS compliance, any web page which is connected to or redirects to a payment capture web page, also needs to be PCI DSS compliant.
   - King's strategy is to outsource this risk to PCI DSS compliant processors or other PCI DSS compliant third parties.
   - No King's hosted website can redirect customers directly to a payment capture page hosted by a PCI compliant processor and the acceptable solution is instead to have a summary page which is hosted by a PCI DSS compliant processor or vendor sitting in between the King's hosted web pages and the payment capture page.

b. The communication between the non-PCI DSS compliant web pages and PCI DSS compliant web pages must be encrypted using TLS 1.2 or higher version.
   - Existing King's web pages can continue to use TLS 1.2.
   - Existing King's web pages using TLS 1.1 or TLS 1.0 or SSL are no longer acceptable and need to be upgraded to TLS 1.2 as a minimum or preferably TLS 1.3as soon as possible.

c. To minimise man-in-the-middle-attacks, a King's web page redirecting to a PCI DSS compliant web page must also comply with the following:
   - The redirect must include a secret passcode, known only by King's and the PSP;

- When the customer is returned to the King's website from the PCI DSS compliant processor, following a successful payment, the King's application must make a server-to-server call to the PSP to validate the payment amount and validate that the transaction receipt number is unique (i.e. has not been used previously);
- Additional mandatory information security requirements for King's websites involved with the payment process:
    - Vendor-supplied defaults always changed;
    - Unnecessary default accounts removed or disabled;
    - All system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches;
    - Critical security patches installed within 14 days of release, in accordance with the KCL Patch Management Policy;
    - All users accessing web servers and associated systems need to be assigned a unique ID and must with administrative or other elevated privileges be authenticated using multi factor authentication (MFA);
    - A minimum password length of at least 12 characters, containing both numeric and alphabetic characters in accordance with the KCL Password Procedures;
    - Group, shared, or generic accounts, passwords, or other authentication methods are prohibited;
    - Administrator access for any terminated users immediately deactivated or removed;
    - Up to date anti-malware software which is updated daily as a minimum;
    - Completion of annual penetration tests and mitigation of any Critical, High and agreed Medium vulnerabilities;
    - Quarterly internal and external network scans and mitigation of any Critical, High and agreed Medium vulnerabilities;
    - Up to date network diagrams;
    - Role based access controls;
    - A maintained inventory of system components that are in scope for PCI DSS;
    - Use of OWASP principles by web developers and peer reviews of any code changes; and
    - Restricted physical access to any physical servers.

6. Card Processing – Chip and PIN Devices

6.1 Using Chip and PIN devices is a very secure way to process card payment transactions. The Chip and PIN devices need to be PCI DSS PTS (PIN Transaction Security) compliant as well as being either PCI P2PE (Point to Point Encryption) certified and/or use GPRS (General Packet Radio Services) encrypted transmission.

6.2 Chip and PIN devices are also known as PEDs (PIN Entry Devices) and PDQs (Process Data Quickly).

6.3 Obtaining a PDQ or PED:

a. Elavon device: Please contact the Finance, Head of Income Services to discuss your requirements.
b. Uniware device: Please contact Uniware (relevant to King's Food only).
c. Zettle device: This has been approved for use by Fundraising only, who need to contact Zettle for any additional devices.

Note: To setup a PDQ device please follow the instructions provided by the applicable vendor that should be included with the PDQ device.

6.4 Customer Present with a payment card: When the customer is present, the card must be processed through a Chip and PIN device according to the device instructions. It is important to consider the positioning of the device to ensure that any in-house CCTV does not record customers entering their card PIN numbers.

6.5 If the transaction is successfully processed, the merchant copy of the payment receipt must be stored and the customer copy given to the customer. The full card number must not be printed on either the King's (merchant) receipt copy or the customer receipt copy. If the full card number is printed it means that the Chip and PIN device has been incorrectly configured and this needs to be raised with the device supplier, who can send a remote fix to the device.

6.6 If the transaction is declined, the customer must be advised immediately. The option of paying with a different card should be offered. The customer receipt copy stating that the payment was declined must be given to the customer and the merchant copy must be stored.

6.7 The PDQ device transaction slips must be reconciled to the PDQ Z report at the end of business each day that payments are taken, and an EReturn submitted via Business World for the appropriate accounting entries. See Income Services intranet page for further details.

6.8 Some customers may provide their card details in writing for processing, i.e. by fax or in a letter. Customers should be deterred from providing the information in this manner (unless explicit approval has been obtained from the Finance, Head of Income Services) as it can be potentially insecure.

7. Safeguarding Chip and PIN Devices

7.1 Once a department has been provided with a Chip and PIN device it is that department's responsibility to ensure its safekeeping at all times, until such time as the device is either returned to Finance or the device supplier. Roles and responsibilities for performing activities in this section 6 of the card payments procedures must therefore be documented, assigned, and understood.

7.2 On receipt of a new device and before it is used, the device's refund and void PIN codes must be changed from the default factory set codes. Knowledge of both codes must be limited to the least number of appropriate staff members needed by the business area in order for the business to operate normally.

7.3 Chip & PIN devices must be secured at all times and must never be left unattended in an open office. Refund and void codes must never be stored with a device or written on or stuck to a device. This is particularly relevant for any section that has a GPRS enabled wireless device which allows the user to carry it around with them. If the office is to be vacated the device must be locked away securely and out of sight where practically possible.

7.4 When a staff member with access to refund codes leaves or moves role, the refund and void PIN codes must be changed.

7.5 It is each section's responsibility to maintain the following security checks for their Chip and PIN devices:

a. To physically check each of their Chip and PIN devices regularly as part of their regular everyday use, as well as official quarterly checks, for signs of tampering or suspected tampering, including:
   - Holes drilled in a device that shouldn't be there
   - Wires and/or devices that are attached to a Chip and PIN device that shouldn't be there
   - Device misbehaving abnormally
   - The device serial number is different from what is logged in the inventory (upon receipt of a device, the serial number for each device needs to be logged)

b. These quarterly Chip and PIN device security checks need to be formally logged
   - Unused devices stored in a secure locked location still need to be checked
   - Records to be retained for at least a six-month period
   - Records to be auditable by an independent assessor

c. Any swap out of a device or receipt of a new device or a return of a device must be organised through and delivered or removed by the supplier of that device. This process needs to be formally logged and Income Services must be informed via: pci-confirmations@kcl.ac.uk
   - Records to be retained for at least a six-month period
   - Validate the person delivering / swapping out the device

d. Any suspicious behaviour around Chip and PIN devices needs to be reported, such as attempts by unknown persons to unplug or open or take away / substitute a device.

e. Report any signs of a Chip and PIN device being tampered with, missing, swapped or any other unexpected or suspicious behaviour around a device to:

   Email: 88888@kcl.ac.uk
   Phone: 020 7848 8888

   Clearly requesting that the ticket raised should be referred to the IT Cyber Security team in the first instance.

f. Training to be provided to all King's staff using Chip and PIN devices includes the following:
   - How to verify third parties who are delivering a new or replacement device;
   - How to check a device for any signs of tampering or unauthorised/unexpected substitution;
   - Identifying and being aware of suspicious behaviour around devices; and
   - How to report signs of tampering and/or suspicious behaviour to the IT Service Desk.

7.6 If unsure of anything in this section you should send an email to PCI-Questions@kcl.ac.uk and someone will be in contact with you to discuss the issue further.

7.7 Further details on the security checks for Chip and PIN devices can be found in the Securing Chip & PIN Devices Procedures document.

8. Phone Payments

8.1 No payment details are to be accepted using the King's telephony system.

8.2 King's business areas are instead, encouraged to make use of approved online payment methods.

8.3 If you believe there to be a strong business case to take payment details over the phone and there is no viable alternative, please contact the Finance, Head of Income Services to discuss further.

9. Use of the eStore

9.1 An alternative approach is to make use of the eStore. The eStore is King's online shop, available for all departments around the university to make use of. The eStore allows a department to have a unique payment page setup for their product, service, conference or event. A direct link to the relevant payment page is provided, which can be sent to the payer and which allows them to make a card payment online, with the relevant accounting entries automatically accounted for in Business World (the King's Finance System).

9.2 This service is available by setting up a product on the King's eStore and further information on eStore can be found at: https://internal.kcl.ac.uk/about/ps/finance/eStore/index

10. Unattended Kiosks and Vending Machines

10.1 No payment details are to be accepted using unattended Kiosks.

10.2 King's business areas are instead, encouraged to make use of approved online payment methods.

10.3 If you believe there to be a strong business case to take payments via unattended Kiosks, please contact the Finance, Head of Income Services to discuss further.

10.4 Any Vending Machines must use PCI DSS compliant payment devices, be initially approved by Finance, Head of Income Services and their compliance needs to be validated annually. Any new vending machines need to go through the King's procurement process.

11. King's Computers used to View or Process card payment transactions

11.1 No payment card data can be either viewed or processed via a King's PC or laptop, where the full payment card number is viewed or keyed.

12. Online Refunds

12.1 Refunds must be approved by the appropriate authorised signatory in accordance with the refund procedures for the College online system being used. The appropriate system is then accessed by the nominated College person(s) and the refund is processed back to the source card from which the original transaction was authorised.

12.2 For College online sites using the PSP Global Payments, refunds can be processed back onto the original source card within 548 days (18 months) of the transaction being taken. For other processors, check before processing a refund what is the acceptable time period for a refund to be processed.

12.3 If in any doubt about the PSP your online system uses, please refer your question to the Finance Head of Income Services.

12.4 The time limits placed on refunds being processed back onto the original source cards are purely as a result of the security measures implemented by the corresponding PSP.

12.5 If outside of the above refund timescales, the customer should be contacted for alternative details for the refund to be processed either by BACS or a bank transfer payment via our Accounts Payable section.

12.6 These refunds are processed via the PSP's online portal and each user needs to have their own Username and Password to log in to a PSP portal.

13. Chip and PIN device Refunds

13.1 Refunds need to be authorised on Chip and PIN devices using a "Supervisor PIN or Password". This PIN / Password must be kept securely by the nominated device users. If currently you do not use a "Supervisor PIN or Password" you need to contact Elavon or your device supplier to arrange to setup a PIN number or password for your device and to restrict its use where refunds are concerned only to the appropriate and necessary users. Also refer to points 7.2 and 7.3.

13.2 Refunds should only be processed through the device back onto the source card from which the original transaction was authorised.

13.3 Refunds must under no circumstances be processed onto a card if the original payment was not processed through your device. Card scheme rules state that refunds must only be processed on a payment card where there is a corresponding sale.

13.4 If the source card is unavailable for the refund to be processed, and only where a valid reason has been provided (e.g card account has since been fully closed), the customer needs to be contacted for alternative details for the refund to be processed by BACS or bank transfer though Accounts Payable. If the customer card has simply been replaced with a new card on the same account due to the original card expiring, any card refund will still credit the correct originating card account.

13.5 The merchant banks King's use to accept card payments also monitor refund transactions and may flag up any refund transaction that contravenes the card scheme rules, i.e. where a refund has been paid to a card without an original corresponding sale.

14. Online Storage of Card Details

14.1 Online storage of card details on King's PC's or servers or databases in any format (email, access databases, excel spreadsheets, pen drives, OneDrive, SharePoint etc.) is strictly forbidden under any circumstance.

14.2 It is important to note that the most common method of fraudsters obtaining card details is by hacking into computers which store cardholder information.

15. Storage of Chip and PIN device Receipts, Chargeback / Dispute documents

15.1 When storing merchant copies of payment receipts and/or chargeback / dispute documents, these must be treated as confidential documents and stored securely, if they include the full card number

15.2 Secure storage is defined as within a safe or within a locked cash box or within a locked drawer, with access provided to authorised individuals only.

15.3 Merchant copies of Chip and PIN devices payment receipts not showing the full card number, can be retained for up to six years after which the receipts must be disposed of via the confidential waste bins or shredded using a cross-cut shredder. Payment card receipts showing the full card number need to be cross shredded immediately.

15.4 Archives and Information Management can provide secure offsite storage of processed receipts in the College's record stores.

15.5 Any new Chip and PIN device receipts must not have the full card number printed on either the customer or merchant receipt copies. Therefore, if a receipt copy does have the full card number printed, this will be a configuration issue, which can be easily corrected by contacting the existing device supplier, which for PDQs is currently Elavon.

16. Compliance and Monitoring

16.1 All payment card processing activities of the College must comply with PCI DSS and the College's Financial Regulations and Procedures and the Data Protection Policy. No activity or technology can obstruct compliance with PCI DSS. All Sections must adhere to this Policy to minimise the risk to both customers and the College.

16.2 As per 10.10.1.3 of the Financial Procedures – where departments require the facility to take card payments, they need to contact the Finance, Head of Income Services initially to make the necessary arrangements. Departments must not make their own arrangements with Payment Services Providers (PSPs).

16.3 Failure to maintain compliance with PCI DSS may render the College liable for fines and may also result in Visa and/or MasterCard prohibiting payment card transactions from being processed by King's.

16.4 The College may screen potential employees to minimise the risk of internal malicious attacks.

16.5 Some PCI compliant Payment Service Providers can be found via the following websites:

www.visa.com/splisting/searchGrsp.do

https://www.mastercard.com/globalrisk/en/resources/pci360.html

16.6 Contact the Finance, Head of Income Services for general enquiries including information on:

a. Making use of the College online eStore
b. Obtaining an office based PDQ device
c. Initial guidance on any out of the ordinary card payment acceptance setups

16.7 If you have any PCI DSS related questions, please use the following email address:

PCI-Questions@kcl.ac.uk