HNC Policies, Protocols and Procedures

Card Payment Policy (including data, data security and refunds)

1. Statement

HNC Finance Office handles sensitive cardholder data daily. Sensitive Data must have adequate safeguards in place to protect it, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

HNC commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end, the College is committed to maintaining a secure environment in which to process cardholder data so that it can meet these promises.

2. Scope

This Policy and Procedure applies to all employees, or agents/ third parties acting on their behalf, in relation to the handling and security of cardholder data, payments and refunds. In addition, the policy shall be referred to in, and follow, the College Financial Regulations.

3. Purpose of the policy

- To protect the data and privacy of all students, staff and other stakeholders of the College
- To maintain a secure environment to process card holder data
- To ensure continuity of service for College staff, students and other stakeholders in the event of a payment system failure
- To ensure the College's compliance with appropriate legislation
- To confirm the College's Refunds Policy in relation to On-line card payments

4. Handling of Cardholder Data

4.1 Employees handling sensitive cardholder data should ensure and bear in mind the following:

- Handle company and card holder data in a manner that fits with their sensitivity
- Protect all cardholder data
- Ensure that passwords and accounts remain secure and are not shared; authorised users remain responsible for the security of their passwords and accounts
- Request approval from management (via the College Systems group) prior to establishing any new software, hardware or third party connection
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended. College devices will automatically move to a password-protected screensaver after 15 minutes
- Report any data security incident, without delay, to the individual responsible for the incident response locally – see the incident response plan
- Ensure that all PIN entry devices are appropriately protected and secured so they cannot be tampered with or altered in any way. Devices will be locked away when there is not a member of the Finance/Student Helpdesk team present e.g. during holiday periods
- Take all necessary steps to prevent unauthorised access to confidential data which includes card holder data
- Delete any sensitive card data that is no longer required by HNC for business reasons in a secure and irrecoverable manner
- Mask any full PAN (Permanent Account Number) when displayed

- Not send card holder data (PAN, track data) over the internet via email, instant chat or any other end user technologies

4.2 Responsibilities of those handling card holder data

- Those handling card holder data each have a responsibility for ensuring the College's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager
- It is required that all employees handling cardholder data confirm that they understand the content of this policy document by signing an acknowledgement form (see Appendix B)

4.3 Storage of card holder data

It is strictly prohibited to store:

- The contents of the payment card magnetic stripe (track data) on any media whatsoever
- The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever
- The PIN or the encrypted PIN Block under any circumstance

4.4 The College will also take the following steps

- Maintain a list of devices that accept payment card data; 1 card machine is located on the Student Helpdesk (LRC) connected to the College wired network. When not in use, this device is kept in the Finance Office
- The inventory of these devices is held by the IT Services Team and includes make, model serial number and location of the device. The list will be updated when and if devices are added, removed or relocated. The Finance team will liaise with the IT Services team if changes are made to the card machines
- Periodically inspect POS device surfaces to detect tampering or substitution
- Train staff using any POS device and make the employees aware of POS handling protocols
- Verify the identity of any person claiming to need to repair, run maintenance tasks on the devices, install new devices or replace devices
- Train staff to report suspicious behaviour and indications of tampering of the devices to the Assistant Principal Finance and Resources
- Restrict access to sensitive cardholder data such as PAN's, personal data and business data only to those employees who have a legitimate need to view such data
- Undertake background checks (such as criminal checks, within the limits of the law) before they commence their employment with the College
- Restrict access to cardholder data according to job role
- Filter e-mail to the College before delivery, however e-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain a virus
- Enable automatic updates for all College devices for system patches released from Microsoft
- The College reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose; more data is contained in the IT Acceptable and Safe Use Policy

5. Methods of 'Electronic Payment'

5.1 HNC accepts 'electronic payments' in the following ways;

- Card payments in person
- Online payments via a third party application (currently Wisepay and SchoolHire)

5.2 Credit/Debit Card Payments in Person

- The card machine is located at the Student helpdesk in the Learning Resource Centre (LRC), connected via the specified network point only
- The Finance Office attached to the LRC or the Student Helpdesk are the only locations in HNC where card payments via a PIN device will be taken
- The machine (s) should not be removed from this location without prior consent from the Assistant Principal Finance and Resources and the Director of IT (Infrastructure & Technical Services)
- Card payments in person should only be taken by a member of the Finance team or the Student Helpdesk team

5.2 Online Payments via a third party application

- All third-party companies providing Online Payment Services to HNC must provide an agreed Service Level Agreement
- All third-party companies which have access to card holder data must:

  a) Adhere to the PCI DSS security requirements, level 1
  b) Acknowledge their responsibility for securing the card holder data
  c) Acknowledge that the card holder data must only be used for assisting the completion of a transaction, supporting a loyalty programme, providing a fraud control service or for uses specifically required by law
  d) Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure
  e) Provide full co-operation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party

5.3 Refunds

- Refunds can be made via Wisepay or SchoolHire by members of the Finance team only using the relevant secure authorisation code
- Refunds can be made in person by members of the Finance team only and students should visit the finance office if a refund is required

6. Roles and Responsibilities

6.1 The Assistant Principal Finance and Resources is responsible for overseeing all aspects of financial regularity, including but not limited to;

- Creating and distributing financial policies and procedures

- Overall responsibility for any online payment system
- Responsibility for the performance and actions of the Finance team

6.2 The Director of IT (Infrastructure and Technical Services) is responsible for overseeing all aspects of data security, including but not limited to;

- Creating and distributing security policies and procedures
- Monitoring and analysing security alerts and distributing data to appropriate data security and business unit management personnel
- Creating and distributing security incident response and escalation procedures that include:
  a) Maintaining a formal security awareness programme for all employees that provide multiple methods of communicating awareness and educating employees
  b) Review handling procedures for sensitive data and hold periodic security awareness meetings to incorporate these procedures into day to day College practice
- Review and update College security policies as needed
- The IT Services team Office shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS. For example, user account maintenance procedures, and log review procedures
- Monitor and analyse security alerts and data, and distribute to appropriate personnel
- Administer user accounts and manage authentication
- Monitor and control all access to data
- Maintain a list of service providers

7. System unavailability response

If there is a suspected payment system failure, the Finance Team must report it to the Assistant Principal Finance and Resources who will liaise with the IT Services team;

- A log of events and system down time will be maintained by the IT Services team and reported to the Finance team, to allow the performance of individual system providers to be monitored
- The IT Services team will advise the relevant Card Payment Provider, or for online payments this is the company that provide the online payments system (currently Wisepay or SchoolHire) and technically liaise with them to resolve the issue
- The IT Services team will keep the Assistant Principal Finance and Resources informed of progress
- In the event of payment systems not being available, the Assistant Principal Finance and Resources will advise College users (staff, students, parents/carers) by email, detailing an alternative method (s) of payment, including the option of cash payment, to ensure business continuity, particularly in relation to trips, visits and lettings
- The Assistant Principal Finance and Resources will keep all stakeholders informed of the expected and actual date of the return of system availability

8. Current asset data and supporting data

Asset/Device Name	Serial Number	Description	Owner/Approved User	Location
HNCMachine2	14323WL80829451	iWL200-01B1328A	Finance and Student Helpdesk Team	Student helpdesk or Finance Office

- No direct connections from the internet to a card holder data environment will be permitted. All traffic has to traverse through a firewall
- Group, shared or generic user account or password or other authentication methods must not be used to administer any system components
- Administrator access to web based management interfaces is encrypted using strong cryptography by the provider of the system
- HNC uses Sophos Central, which is configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems
- All removable media (for example floppy and others) is scanned for viruses before being used although use of such items is discouraged
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline
- End users are not be able to modify and any settings or alter the antivirus software
- All workstations, servers, software, system components etc. owned by HNC have up-to-date system security patches installed to protect the asset from known vulnerabilities

9. Review of policy and communication

The Senior Leadership Team will review and approve the policy, and the Finance and Resources Committee will receive the policy for information. Once approved, the policy will be published on the College's website. The policy will be reviewed every three years or as required by changes in legislation.

v.	Date	Author(s)	Comments	Approval Route/ Date	Date of Next Review
1	2016	Andrew Shaw, Rebecca Sutcliffe, Julie Pryce	Introduced as the College introduced card payments	SLT 2016 F & R Committee for data only	As required
2	November 2021	John Flynn, Rebecca Harris, Julie Thomas	Updated staffing and location of card payment machine	SLT 1/12/2021 F & R Committee for information only	Triennially June 2024

Appendix A: Incident Response Plan

The College PCI Security Incident Response Team:

Assistant Principal Finance and Resources
Director of IT (Infrastructure and Network Services)
Vice Principal Corporate Services and Planning Finance
Manager
Online Payment companies Internal
Audit as appropriate College
bankers
Relevant Credit/ Debit card companies

'Security incident' means any incident (accidental, intentional or deliberate) relating to our communications or data processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal data or money, or to damage the College.

The HNC PCI security incident response plan is as follows:

- If there is a suspected data security breach, the Finance Team must report it to the Director of IT (Infrastructure and Network Services)
- The IT Services team will investigate the breach and limit the exposure of card holder data, mitigating the risks associated with the incident
- The IT Services team will inform the Assistant principal Finance and Resources, who will determine the nature of the incident and follow relevant guidance
- The IT Services team will ensure compromised systems are isolated on/from the network
- The IT Services team will gather, review and analyse the logs and related data from various central safeguards and security controls
- The Assistant Principal Finance and Resources and the Director of IT (Infrastructure & Technical Services) will make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required
- The Assistant Principal Finance and Resources and the Director of IT (Infrastructure & Technical Services) will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred

Appendix B: Employee Agreement to Comply With Payment Policies

_____

Employee Name (printed)

I agree to take all reasonable precautions to assure that company internal data, or data that has been entrusted to the HNC by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Company, I agree to return all data to which I have had access as a result of my position. I understand that I am not authorised to use sensitive data for my own purposes, nor am I at liberty to provide this data to third parties without the express written consent of the internal manager who is the designated data owner.

I have access to a copy of the Card Payment Policy, I have read and understand this policy, and I understand how it impacts my role responsibilities. As a condition of continued employment, I agree to abide by the policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of the payments policy to the Assistant Principal Finance and Resources.

_____

Employee Signature

_____

Date

Question	Response
1. Name of policy being assessed	Card Payment Policy
2. Summary of aims and objectives of the policy	HNC commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end, the College is committed to maintaining a secure environment in which to process cardholder data so that it can meet these promises.
3. What involvement and consultation has been done in relation to this policy? *(e.g. with relevant groups and stakeholders)*	The Policy has been previously approved by the Senior Leadership Team. The policy has been reviewed and updated with content being benchmarked against current best practice.
4. Who is affected by the policy?	HNC Stakeholders
5. What are the arrangements for monitoring and reviewing the actual impact of the policy?	Triennially, in response to legislative changes or in the event of a security incident.

Protected Characteristic Group	Is there a potential for positive/negative impact?	Please explain and give examples of any evidence/data used	Action to address negative impact (e.g. adjustment made)
Disability	Neutral impact	The policy is compliant with all regulations and guidance and undergoes periodic review to ensure it remains up to date and fit for purpose.	N/A
Gender reassignment	Neutral impact	The policy is compliant with all regulations and guidance and undergoes periodic review to ensure it remains up to date and fit for purpose.	N/A
Marriage or civil partnership	Neutral impact	The policy is compliant with all regulations and guidance and undergoes periodic review to ensure it remains up to date and fit for purpose.	N/A
Pregnancy and maternity	Neutral impact	The policy is compliant with all regulations and guidance and undergoes periodic review to ensure it remains up to date and fit for purpose.	N/A
Race	Neutral impact	The policy is compliant with all regulations and guidance and	N/A

		undergoes periodic review to ensure it remains up to date and fit for purpose.	
Religion or belief	Neutral impact	The policy is compliant with all regulations and guidance and undergoes periodic review to ensure it remains up to date and fit for purpose.	N/A
Sexual orientation	Neutral impact	The policy is compliant with all regulations and guidance and undergoes periodic review to ensure it remains up to date and fit for purpose.	N/A
Sex (gender)	Neutral impact	The policy is compliant with all regulations and guidance and undergoes periodic review to ensure it remains up to date and fit for purpose.	N/A
Age	Neutral impact	The policy is compliant with all regulations and guidance and undergoes periodic review to ensure it remains up to date and fit for purpose.	N/A

Evaluation:

Question	**Explanation / justification**	
Is it possible the proposed policy could discriminate or unfairly disadvantage people?	The policy ensures a transparent setting of expectations; no discrimination or disadvantage could be displayed	
Final Decision:	**Tick the relevant box**	**Include any explanation / justification required**
1. No barriers identified, therefore activity will **proceed**.	√	Intelligence related to GDPR, IT and FE best practice and guidance. Experience of DPO and Data Security group has a positive impact on this policy.
2. You can decide to **stop** the policy or practice at some point because the data shows bias towards one or more groups		
3. You can **adapt or change** the policy in a way which you think will eliminate the bias		

4. Barriers and impact identified, however having considered all available options carefully, there appear to be no other proportionate ways to achieve the aim of the policy or practice (e.g. in extreme cases or where positive action is taken). Therefore you are going to **proceed with caution** with this policy or practice knowing that it may favour some people less than others, providing justification for this decision		

Reviewed by (Author):	John Flynn
Date:	30th November 2021
Review date (if applicable):	2024
Approval by (SLT Lead):	Julie Thomas
Date:	30th November 2021