Huddersfield New College Further Education Corporation

Card Payments Policy (including information security and refunds)

1.0 Policy Statement

Huddersfield New College Finance Office handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Huddersfield New College 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 information so that it can meet these promises.

2.0 Scope

This Policy and Procedure applies to all employees, or agents/ third parties acting on their behalf, in relation to the handling/ security of cardholder data, payments and refunds.

In addition, the policy shall be referred to in and follow the College Financial Regulations.

3.0 Purpose of the Procedure

- To protect data and privacy of all students, staff and other stakeholders of the College.
- To maintain a secure environment to process card holder information.
- To ensure the College's compliance with appropriate legislation.
- To confirm the College's Refunds Policy in relation to Online card payments

4.0 Access to the Policy and Procedure

This policy is accessible via the College's website and is also available on request from the Assistant Principal (Finance). The policy is available in alternative formats on request to the Assistant Principal (Finance).

5.0 Review of Policy

5.1 The policy shall be reviewed at least every 2 years by the College Senior Leadership Team.

5.2 Date of next Review: February 2018

6.0 Handling of Cardholder Data

6.1 Employees handling Sensitive cardholder data should ensure/ bear in mind the following:

- They handle Company and cardholder information in a manner that fits with their sensitivity;
- Huddersfield New College reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure
- Not share accounts;
- Authorised users are responsible for the security of their passwords and accounts.
- Request approval via the college systems group prior to establishing any new software or hardware or third party connections.
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended, college PCs will automatically go to a password-protected screensaver after 15 minutes.
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – see incident response plan.
- All PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered, they should be locked away when there is not a member of the Finance team present e.g holiday periods.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Any sensitive card data that is no longer required by Huddersfield New College for business reasons must be discarded in a secure and irrecoverable manner
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed
- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- Visitors must always be escorted by a trusted employee when working in the Finance Office, if contractors need to work unattended then the card machines must be put away in the safe and PCs locked.
- A list of devices that accept payment card data should be maintained, 2 Card Machines are located in the Finance Office, connect via ISDN line, the inventory of these devices is held by the IT Support Team and includes make, model serial number and location of the device. The list will be updated when devices are added, removed or relocated. The Finance team must liaise with the IT Support team if changes are made to the card machines.
- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the College.

- The job description of the user determines the level of access the employee has to cardholder data

6.2 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 information confirm that they understand the content of this policy document by signing an acknowledgement form (see Appendix A)

6.3 Storage of Cardholder 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.

7.0 Methods of 'Electronic Payment'

7.1 Huddersfield New College accepts 'electronic payments' in the following ways:-

- Credit/ Debit Card Payments in Person to the College
- Credit/ Debit Card Payments over the Phone to the College
- Online Payments to the College via a third party application
- Card payments to third party organisations via College media (eg, College caterers)

7.2 Credit/ Debit Card Payments in Person

- 2 Card Machines are located in the Finance Office, connect via ISDN line.
- The 'Finance Office' is the only location at Huddersfield New College where card payments via a PIN device will be taken for Huddersfield New College.
- The machines should not be removed from this location without prior consent from the Assistant Principal (Finance) and the IT Network Manager
- Card payments in person should only be taken by a member of Finance team, currently Meena Gill or Sharon Littler
- In addition, Exam Resit payments can be taken in person by an assigned member of staff working in the Finance Office only. Prior notification of dates and staff member assigned to this duty must be given to the Assistant Principal (Finance) and the IT Network Manager so training and any access needed can be granted.

7.3 Credit/ Debit Card Payments over the Phone

- The Finance Office is the only location at Huddersfield New College where card payments will be taken over the phone for the College
- The Business Manager secure web service provided by Worldpay is the only way in which a card payment can be taken over the phone at Huddersfield New College. No cardholder data must be written down, it must be input directly into the Online Application.
- Card payments over the phone should only be taken by a member of the Finance Office Team using their assigned account for the Business Manager.
- In addition, Exam Resit payments can be taken in person by an assigned member of staff working in the Finance Office only. Prior notification of dates and staff member assigned to this duty must be given to the Assistant Principal (Finance) and the IT Network Manager so training and any access needed can be granted.
- The Online Application should only be used on the fixed PCs in the Finance Office to take payments over the phone. Use of the Application outside of this area is strictly prohibited, including on remote access to college systems.

7.4 Online Payments via a third party application, &
Card payments to third party organisations via College media

- All third-party companies providing Online Payment Services to Huddersfield New College or for/ to whom payments are received on behalf of Huddersfield New College must provide an agreed Service Level Agreement.
- All third-party companies which have access to Card Holder information must:

1. Adhere to the PCI DSS security requirements at level 1.
2. Acknowledge their responsibility for securing the Card Holder data.
3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
5. Provide full cooperation 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.

8.0 Roles and Responsibilities

8.1 The Assistant Principal (Finance) is responsible for:

- overseeing all aspects of information security, including but not limited to:
- Creating and distributing security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and College management personnel.
- creating and distributing security incident response and escalation procedures that include maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).

8.2 The IT Network 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).

8.3 Finance Office Administrators shall:

- Monitor and analyse security alerts and information and notify the Assistant Principal (Finance) and the IT Network Manager
- Administer user accounts and manage authentication
- Monitor and control all access to data.
- Maintain a list of service providers.

Appendix A: Security procedures

1. Disposal of Stored Data

- All data must be securely disposed of when no longer required by College, regardless of the media or application type on which it is stored. (Data up to 6 years old may need to be maintained for audit purposes),
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- The College will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- The College will have documented procedures for the destruction of electronic media. These will require:
    - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in a lockable storage container/ area clearly marked "To Be Shredded" - access to these containers must be restricted to Finance Office staff.

2. Security Awareness and Procedures

- The review of handling procedures for sensitive information and the holding of periodic security awareness meetings will be incorporated into day to day College practice procedures.
- College security policies will be reviewed annually and updated as needed.

3. Information Supporting Policy

- No direct connections from Internet to cardholder 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.
- Huddersfield New College uses Symantec Endpoint Protection, 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 any settings or alter the antivirus software
- All Workstations, servers, software, system components etc. owned by Huddersfield New College must have up-to-date system security patches installed to protect the asset from known vulnerabilities.

Appendix B: Incident Response Plan

Associated college policies are:

- E-safety, IT security and electronic communications policy (soon to be replaced by separate IT Acceptable Usage & E-Safety Policy)
- Password Policy.

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

Huddersfield New College PCI security incident response plan is as follows:

1. If there is a suspected security breach/incident the Finance Team must report it to the Assistant Principal (Finance) and the IT Network Manager for any security related issues.
2. That member of the team receiving the report will advise the relevant Card Payment Provide. For Card Payments in person or over the phone this is WorldPay though Yorkshire Bank, for online payments this is the company that provide the online payments system.
3. That member of the team receiving the report will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
4. That member of the team receiving the report will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. That member of the team receiving the report 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, or for the institution.
6. Ensure compromised system/s is isolated on/from the network.
7. Gather, review and analyse the logs and related information from various central and local safeguards and security controls
8. Conduct appropriate forensic analysis of compromised system.
9. Inform the Principal as required
10. Involve/ inform the Audit Committee of the Corporation/ internal and/ or external auditors as appropriate
11. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
12. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

Credit/ Debit card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data by contacting relevant parties.

The College PCI Security Incident Response Team:

Principal
Assistant Principal (Finance)
IT Network Manager
Finance Office Manager
(as needed)
Online Application
Internal Audit
College bankers
Relevant Credit/ Debit card companies

Appendix C – Employee Agreement to Comply Form

_____

Employee Name

_____

Job title

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

I have access to a copy of the Payments Policy, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the College security policy. I understand that non-compliance could be cause for disciplinary action, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of payments policy to the Assistant Principal (Finance) & IT Network Manager.

_____

Employee Signature

Appendix D – Current Asset Information

Asset/Device Name	HNCPDQ01 Base Unit	HNCPDQ01 Handheld Unit
Model	iWL200-01B1328A	IWL252-01T1467A
Serial Number	14324IWL80832235	14324WL80830576
MAC Address	54 7f 54 f6 5c 96	N/A
TID Number (Terminal ID)	N/A	26958702
Approved User	Finance Team	Finance Team
Authorised Location	Finance Office	Finance Office
Asset/Device Name	**HNCPDQ02 Base Unit**	**HNCPDQ02 Handheld Unit**
Model	iWL200-01B1328A	IWL252-01T1467A
Serial Number	14324IWL80831783	14323WL80829451
MAC Address	54 7f 54 f6 5b c0	N/A
TID Number (Terminal ID)	N/A	26958701
Approved User	Finance Team	Finance Team
Authorised Location	Finance Office	Finance Office

Appendix E: Payment terms and conditions for users of Online payment facilities, including Refund Policy.

Please read these terms carefully before using the online payment facility. By using the online payment facility on this website you accept these terms and conditions.

Conditions

All payments are subject to the following conditions:

- You warrant that in using the online payment facility you are authorised to use the debit or credit card for the payment or payments you are making.
- The College cannot accept liability for a payment not reaching the correct account due to you providing an incorrect account number or other incorrect details whether personal or otherwise.
- The College cannot accept liability for a payment not reaching the correct account where payment is refused or declined by the Card Supplier for any reason.
- If the card supplier declines payment, the College is under no obligation to bring this to your attention. It is your responsibility to check with the Card Supplier that payment has been deducted from the debit or credit account.
- The College will not be liable for any damages arising out of the use, inability to use, or the results of use of this site, any websites linked to this site, or the materials or information contained at any or all such sites, whether based on warranty, contract, tort, delict or any other legal theory and whether or not advised of the possibility of such damages.

By accepting these terms and conditions, you authorise the College to charge the debit or credit card account you have provided for the goods or services required. You agree that there will either be sufficient availability under the credit card limit or sufficient funds in the debit card account to make the card payment at the time of purchase.

Refund policy

Refunds for online payments are at the discretion of the College, and may not be available if stated for with the reason. Refunds may be made for trips/ visits organised by the College if:

- The student leaves the College
- The student leaves their course
- The student is unable to attend due to illness, etc.
- There are enough students on the trip, visit or event waiting list to take the current student's place.

In addition, refunds for other online payments for goods/ services will be made for non-receipt of those goods or services, or where the goods are faulty or mis-described, as covered by the Consumer Rights Acts 2015.

For further information about a refund, please contact our finance department at Huddersfield New College by telephone on 01484 652341 or send an email to info@huddnewcoll.ac.uk as soon as possible.

Refunds, if appropriate, will be processed within 10 working days of the request.

Security

All online payments are through Online World Pay and are encrypted, safe and secure.