What is PCI DSS?
The Payment Card Industry Data Security Standards (PCI DSS) are the minimum Standards of security required to safeguard payment card transactions. The PCI Security Standards Council, who are responsible for ensuring the standards remain relevant as technology evolves, created these Standards. With the current version of the standards issued in May 2018 being v3.2.1. The University is contractually obliged, through our acquirer Global Payments, to obtain PCI DSS compliance. By maintaining the standards, we reduce the risk of exposure to payment card fraud for our students, staff and customers.

What is a Card Not Present (CNP) transaction?
The term ‘card not present’ is used for a payment made by a customer where the customer and their payment card are not present at the point of sale. The card details are provided via phone call, using an analogue phone line, or in exceptional circumstances by mail. Card details can never be accepted by email or other electronic communication means as the data would not be secure at the required standard. At the University, CNP transactions are processed using a Payment device (sometimes known as a PED or PDQ).

What do I need to do?
- Complete a daily visual check of the devices to ensure they have not been tampered with. Complete the daily log as evidence of review.
- Ensure payment card information is only taken over an approved phone line.
- Ensure the card number is input directly into the PDQ terminal. The payment card data must not be written down.
- Ensure the receipts only print the last four digits of the customer’s card number. This is referred to as the card number being truncated.
- Ensure supervisor passwords are only known to supervisors and passwords are changed at a minimum when staff changes occur.
- Ensure the device is always visible to a team member.
- Ensure the device is stored in a secure location when not in use or cannot be observed.
- Where approval has been given for payment card data to be received by mail ensure the SOP’s are followed.

Awareness is key!
- Look out for unusual behavior around the device.
- When taking payment card data over the phone, do not repeat the card number back if you are in an open environment. Ask the customer to repeat the number.
- Never receive or send card details by electronic message or email.
- Challenge visitors to your department, requesting review, access or to swap out any of your payment devices. Ask to see ID/Credentials.

Respond to concerns.
- If you suspect something is wrong, notify your supervisor/line manager immediately.
- Do not use the device, and let others know not to use it.
- For concerns with a device integrated with a till please contact Aman Chana A.S.Chana@warwick.ac.uk
- For concerns with a standalone device please contact Donna Johnson D.E.Johnson@warwick.ac.uk
- Ensure your query/concern has also been logged with the IT helpdesk.

For more information, please refer to the University’s Payment Card Data Security Policy or the PED/PDQ user guide.