GLOVER & HOWE PCI SECURITY PROCEDURES POLICY

APRIL 2021(ANNUALLY REVIEWED)

Payment Card Security Policy and Procedures

Adherence to this policy and the associated procedures is mandatory for all staff who handle or process card payments on behalf of the Glover & Howe Insurance Services.

1. Introduction and Policy Statement

1.1 Glover & Howe preferred method for taking individual payments for insurance services from clients (the customer) payment card (debit or credit card) via Opayo Gateway & Global Payments.

1.2 All cards are transacted on the card gate way and no longer via the portal card machine.

1.3 The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard, created to help organisations that process card payments prevent card fraud. It requires strict control of data and confidentiality to ensure the security of payment card details. It is the global data security standard that any business of any size must adhere to if it wishes to accept card payments, and to store, process, and/or transmit cardholder data. Glover and Howe is liable for fines should it fail to comply with PCI DSS as itis considered a breach of contract with our Bank. Non-compliance also puts confidential data held by the Glover & Howe at potential risk in contravention of Glover and Howe Data protection policy. Protection Policy (available on request)

1.4 Glover & Howe senior management are responsible for ensuring staff area ware of this policy, the associated procedures and that these are adhered to. Mandatory training is provided and should be undertaken annually by staff handling payment card transactions.

1.5 If any member of staff identifies that this policy is compromised or is at risk of compromise then he/she must report the matter immediately to their line manager. They should feel able to do so in the case of genuine mistakes as well as if they are concerned about poor practice by others. The Senior management of Glover & Howe and Directors will decide on whether a further investigation is required.

1.6 Individual staff who do not comply with the requirements of the training and this set of policies and procedures may be subject to disciplinary action.

2. Online Payments

2.1 The preferred method of taking payment for services is via telephone 01206 814500 and transacted on the secure gateway terminal facility.

2.2 If at all possible, payments should be taken by directing the individual to use one of the services above and staff will not therefore have any access to the individual's payment card details.

2.3 Glover & Howe will not activity promote the facility of paying by card but will offer other options of online and cheque payment.

2.4 Through the online payment system no card details are retained by Glover & Howe and there is no access to full card details by any member of staff as this information is stored on an encrypted external server maintained by the online payments service provider Opayo & Global Payments.

2.5 Refunds can only be processed by the designated service for that online payment system stated in paragraph 2.1.

2.6 The Glover & Howe approved supplier for all online payments is Opayo & Global Payments.

3. Card Payments

3.1 All card payments are taking using the online payment no PDQ machines are now in service.

3.2 Payments receipts when requested are either emailed or sent in the post. No hard copy of this receipt is retained at the GH offices.

3.3 If the transaction is declined, the customer should be informed immediately and asked to contact the card provider. Receipts should be handled in the same way as in 3.2.

3.4 If the customer is present then they must be directed to an operator that can submit their details via the secure online platform.

3.5 Confidential and sensitive information (e.g. card numbers) is never to be sent unencrypted through end-user messaging technologies such as e-mail, instant messaging, or chat) Card details should never be requested via email. On no account should card details be processed if received this way. Emails must be deleted out of the inbox and deleted folder and a new message composed to the customer informing them that their card details will not be accepted via email. Please follow the processes in the PCI Awareness Document on LEARN on how to delete the emails.

3.6 Card details should never be requested via a paper booking/payment form.

3.7 All confidential and sensitive data will be retained only if required for legal, regulatory, and business requirements and in a secured location (e.g. locked cabinet/safe). Cardholder “authorization data”, including track, CV2, and PIN information will be retained only until completion of the authorization of a transaction. After authorization, the data must be destroyed via cross shredding or pulping by using GH approved confidential waste service. Storage of cardholder authentication data post-authorization is prohibited.

3.8 All card details are retained by the gateway host Opayo & Global Payments. No card details are to be kept at the GH offices after the transaction has been automated.

3.9 Refunds can only be processed by the staff member authorized to do so by GH approved staff.

3.10 GH credit/debit cards must be stored in a securely locked drawer/cabinet out of sight and only used by the authorised staff member detailed in 3.10 above.

4. Compliance and Review

4.1 The GH will undertake a PCI-DSS Compliance review on an annual basis. Any changes to practice must be fully in line with PCI regulation.

4.2 Members of the PCI-DSS team will do annual and ad hoc spot checks on staff conducting payment online transactions.

4.3 All third-party suppliers who provide card payment facilities must provide the PCI Team with an up to date copy of their Compliance to PCI DSS, on an annual basis.

4.4 GH will carry out regular vulnerability testing on the University network and the results will be notified to the PCI DSS Team.

4.5 The durell (GH IT) regularly update anti-virus software to protect the GH network and its personal computers.

4.6 A GH managed windows desktop must be used to access systems via durell connected to the Card Data Environment (e.g. back office of e-payment facilities). Staff must never use a personal computer.

4.7 All individuals handling card data are expected to comply with all other GH policies which cover security of data.