CRANLEIGH
EX CULTU ROBUR

PAYMENT CARD INFORMATION SECURITY POLICY

INTRODUCTION

This Payment Card Information Security Policy outlines Cranleigh School's and Cranleigh Enterprises Ltd’s standards and procedures for storing and processing payment card data to ensure the protection of cardholder data and to ensure their compliance with the Payment Card Industry Data Security Standard (PCI DSS) and the Data Protection Act 2018.

Reference to Cranleigh School in this policy includes reference to Cranleigh Enterprises Ltd.

This policy applies to all staff members, temporary staff and third party contractors who handle payment card information on behalf of Cranleigh School.

The Governors have delegated responsibility to the Director of Finance for ensuring compliance with the PCI DSS and the School's own guidelines for the management of card payment data.

SCOPE

Cranleigh School operates seven card terminals, one in the School Shop, one in the Reception of the Sports Centre, one in Gatleys café, and four terminals that are held by the Finance Department for use at school functions. Five terminals are provided by AIB Merchant Services and two by SumUp, and operate over a separate network to the School’s main IT systems. The machines offer merchant-approved point to point encryption through external ISDN lines and only limited staff have authorisation and training to use them. Physical access to them is restricted when buildings are not in use by locks and alarms. For clarity, only these Merchant devices and their associated users fall within scope for compliance with PCI DSS.

A SECURE NETWORK FOR CARDHOLDER DATA

Cranleigh School provides a secure network for processing cardholder data as detailed in the Scope by only using Merchant Services devices with end-to-end encryption over a separate network to the main School IT system. No Cardholder information is entered into any IT systems on the School network.

PROTECTING CARDHOLDER DATA

Cranleigh School will not store any payment card data in electronic format including within spreadsheets, word-processed documents or in any information management systems. Cranleigh School will not record phone calls where cardholder data is provided or write down any card details.

For clarity, Cranleigh School does not store any of the following:

- Full magnetic stripe - track 2
- Card Security Code (CSC) otherwise known as Card Verification Code (CVC or CVC2), Card Verification Value (CVV2) or Card Identification Number (CID)
- PIN/PIN block
- Sensitive authentication data (even if it is encrypted)
- All digits of the credit card account number. Only the last four numbers are visible to selected Cranleigh School staff in any form - when the full number needs to be displayed the remaining numbers are always concealed or disguised using other characters (such as '*')

Cranleigh School does not transfer cardholder data over the internet or via any online medium.

If Cranleigh School is required, in a specific (and likely to be rare) circumstance, to transport cardholder data from one location to another, this will always be authorised by the Director of Finance and transported via a secure courier service. All data will have been subject to an inventory check before it leaves the school premises.

VULNERABILITY MANAGEMENT PROGRAMME

Cranleigh School comply with any Merchant Services recommendations to update hardware or firmware on endpoint devices as part of its ongoing commitment to maintaining secure IT systems within the school.

STRONG ACCESS CONTROL MEASURES

Cranleigh School restricts the use of card payment facilities to authorised staff members only.

Authorised staff members are given access to restricted areas containing information systems because they have a justified and approved Cranleigh School business need. The IT security expectations of authorised staff are defined within their individual job descriptions and all staff are required to keep as confidential any information made available. Non-authorised staff members are not permitted to access cardholder data.

Cranleigh School’s card payment facilities are protected to limit access and for wider operational security.

Card machines are inspected daily before use for signs of tampering, eg unexpected attachments or cables plugged into the devices, as well as any physical changes that may indicate that the card machine has been tampered with.

Access to card machines must not be granted to third parties claiming to be maintenance personnel without their identity being verified. Any suspicious behavior must be reported.

An inventory of all card machines is maintained, detailing location, make, model and serial number. Serial numbers of devices are periodically inspected.

REGULAR MONITORING AND TESTING OF NETWORKS

Cranleigh School takes its responsibility for processing cardholder data seriously and regularly monitors all access to its networks and data storage facilities.

The school has an action plan in place designed to minimise any risks to cardholder data. It also maintains a risk register which is reviewed at regular Governing Body meetings or whenever there have been significant changes to risk.

SECURITY INCIDENT MANAGEMENT PLAN

All information security incidents are reported to the Director of IT in the first instance who has delegated responsibility from the Board of Governors for minimising any impact from the incident. Any security breaches or loss of data will be immediately investigated to identify the reasons for the incident and the action needed to resolve any security issues. Cranleigh School's Senior Management Team will be alerted to any security breaches and a process will be put in place to inform any other parties (where relevant) of the security issue.

In the unlikely event that Cranleigh School experiences a security breach it will:

1. Immediately shut down the relevant system or process to prevent any further security breaches.
2. Inform all affected parties (as above) and Cranleigh School's merchant bank provider AIB Merchant Services and SumUp who will immediately initiate their own controls, and the Police.

MAINTAINING AN INFORMATION SECURITY POLICY

Cranleigh School regularly reviews this payment card information security policy to ensure it is in compliance with the PCI DSS.

Last Reviewed: June 2024

STAFF DECLARATION

By signing my name below, I confirm that I have read and understood this policy for the use and security of cardholder data.

NAME	DATE	DEPARTMENT	SIGNATURE