Information Security Policy – Debit & Credit Cards

Conway Primary School

(Company Name)

07th September 2020

(Date)

Contents

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2. Information Security Policy

Conway Primary School 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.

Conway Primary School commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling Sensitive cardholder data should ensure

- Handle Company and cardholder information in a manner that fits with their sensitivity;
- Limit personal use of Conway Primary School information and telecommunication systems and ensure it doesn't interfere with your job performance;
- Conway Primary School reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;

- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our company'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.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Conway Primary Schools established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Conway Primary School will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Conway Primary School unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non compliance.

5. Protect Stored Data

All sensitive cardholder data stored and handled by Conway Primary School and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the company for business reasons must be discarded in a secure and irrecoverable manner.

It is strictly prohibited to store:

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

6. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level:

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Conway Primary School if disclosed or modified. **Confidential data includes cardholder data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure;
- **Public data** is information that may be freely disseminated.

7. Access to the sensitive cardholder data:

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- 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.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
- Conway Primary School will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- Conway Primary School will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- The company will have a process in place to monitor the PCI DSS compliance status of the Service provider.

8. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on Conway Primary School sites. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

9. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.
- Encryption technologies like SSL, TLS, SSH, IPSEC etc. must be used to secure communications in transit of classified information, particularly authentication credentials and the transmission of sensitive information. It can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols.
- Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the

basis for encryption technologies. These algorithms represent the actual cipher used for an approved application.

- Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength.

- Conway Primary School key length requirements will be reviewed annually and upgraded as technologyallows. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec.

- Confidentiality and authentication to wireless networks should be protected by WPA2.

Key Management

- Since security is primarily based on the encryption keys, effective key management is crucial. Effective key management is based on an agreed set of standards, procedures, and secure methods and are characterised by the following precautions:

- ❑ Key management is and must be fully automated (e.g. personnel do not have the opportunity to expose a key or influence the key creation).

- ❑ Key must not appear unencrypted.

- ❑ Keys must contain a random chosen component from the entire key space, preferably by hardware.

- ❑ Key-encrypting keys must be separate from data keys. Data must not appear in clear text that was encrypted using a key-encrypting key.

- ❑ All patterns in clear text are disguised before encrypting.

- ❑ Keys with a long life must be used sparsely. The more a key is used, the greater the opportunity for an attacker to discover the key.

- ❑ Keys must be changed frequently. The cost of changing keys rises linearly while the cost of attacking the keys rises exponentially. Therefore, all other factors being equal, changing keys increases the effective key length of an algorithm.

- ❑ Keys transmission must be secure to well-authenticated parties.

- ❑ Key generating equipment must be physically and logically secure from construction through receipt, installation, operation, and removal from service.

Key Usage

- In general, a single key should be used for only one purpose (e.g. encryption, authentication, key wrapping, random number generation, or digital signatures). There are reasons for this:

1. The use of the same key for two different cryptographic processes may weaken the security provided by one or both of the processes.

2. Limiting the use of a key limits the damage that could be done if the key is compromised.

3. Some uses of keys interfere with each other. For example, consider a key pair used for both key transport and digital signatures. In this case the private key is used as both a private key transport key to decrypt data encryption keys and a private signature key to apply digital signatures. It may be necessary to retain the private key transport key beyond the crypto period of the corresponding public key transport key in order to decrypt the data encryption keys needed to access encrypted data. On the other hand, the private signature key should be destroyed at the expiration of its crypto period to prevent its compromise. In this example, the longevity requirements for the private key transport key and the private digital signature key contradict each other.

- This principle does not preclude using a single key in cases where the same process can provide multiple services. This is the case, for example, when a digital signature provides nonrepudiation, authentication and integrity protection using a single digital signature, or when a single symmetric data encryption key can be used to encrypt and authenticate data in a single cryptographic operation (e.g. using an authenticated encryption operation, as opposed to separate encryption and authentication operations)

10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by Conway Primary School, regardless of the media or application type on which it is stored.
- 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.
- Conway Primary School 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.
- Conway Primary School 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 lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a

high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A)
- 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 company.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

12. Security Management / Incident Response Plan

Employees of the company will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within the company and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Incident Response Plan

1. In the event of a suspected security breach, alert the information security officer or your line manager immediately.
2. The security officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

13. Network security

- Stateful Firewall technology must be implemented where the Internet enters the Conway Primary School Card network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.

- All inbound network traffic is blocked by default, unless explicitly allowed which have to be documented along with a business reason for allowing such access.

- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.

- The firewall rules will be reviewed on a six months basis to ensure validity.

- A separate network segment must be implemented for wireless devices and users, where they are authenticated and firewalled as if they were coming in from the Internet.

- A personal firewall must be installed on a desktop/laptop/mobile device with a user-focused operating system such as Microsoft Windows Vista or Macintosh OS X. A personal firewall provides an additional layer of security for PCs located both inside and outside perimeter firewalls (e.g., mobile laptop users), because it can restrict inbound communications and can often limit outbound communications as well. This not only allows personal firewalls to protect PCs from incoming attacks, but also limits the spread of malware from infected PCs and the use of unauthorized software such as peer-to-peer file sharing utilities.

- Management of personal firewalls should be centralized if at all possible to help efficiently create, distribute, and enforce policies for all users and groups. Any warning messages that are generated by the firewall should be shown to the user of the PC to help them rectify problems that are found

14. Systems Configuration and Password Policy

All users, including contractors and vendors with access to Conway Primary School systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- All vendor default accounts and passwords have to be changed at the time of provisioning the system/device on Conway Primary School network.

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.

- Where SNMP is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.

- For non-console administrative access prevent the usage of insecure technologies like telnet etc. and use appropriate technologies like ssh,vpn,ssl etc

15. Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by Conway Primary School. The preferred application to use is lgfl.net Anti-Virus software, this anti-virus software must be active all the time and must be configured to perform on-access real-time checks on all executed files and scheduled virus checks at pre-set regular intervals and also have to retrieve the latest updates to the antiviral program automatically on a daily basis.
- Conway Primary School Management/Master anti-virus server is scheduled to check the lgfl.net update site every one hour for updates and to auto update both the virus definition file and the software version. Conway Primary School lgfl.net client configuration is set to check the Management/Master server on a daily basis for updates and to auto update and report success and failures. Conway Primary School invest adequate efforts to identify Conway clients who did not attempt to update their virus definitions file for more than 1 month and will take appropriate remedial actions

- 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 virus.

- All removable media (for example floppy and others) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements and for a minimum of 90 days online and 1 year offline.

16. Patch Management Policy

- All Workstations, servers, software, system components etc. owned by Conway Primary School must have up-to-date system security patches installed to protect the asset from known vulnerabilities.

- Where ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from the respective vendor.

- Any exceptions to this process have to be documented.

17. Remote Access policy

- It is the responsibility of Conway Primary School employees, contractors, vendors and agents with
  remote access privileges to Conway Primary School corporate network to ensure that their remote
  access connection is given the same consideration as the user's on-site connection to Conway Primary School Secure remote access must be strictly controlled. Control should be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.

- All hosts that are connected to Conway Primary School internal networks via remote access technologies must be monitored on a regular basis.

- All remote access accounts used by vendors or 3rd parties must be reconciled at regular interviews and the accounts be revoked if there is no further business justification for such access.

18. Wireless Policy

- Installation or use of any wireless device or wireless network intended to be used to connect to any of the Conway Primary School networks or environments is prohibited. If the need arises to use wireless technology it should be approved by Conway Primary School
- Usage of appropriate testing using tools like net stumbler, kismet etc. must be performed on a quarterly basis to ensure that:
  - no wireless devices or networks have been deployed;
  - Any devices which support wireless communication remain disabled or decommissioned.

- If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the Conway Primary School has the authorisation to stop, cease, shut down, and remove the offending device immediately.

19. Vulnerability Management Policy

- As part of the PCI-DSS Compliance requirements, Conway Primary School will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

- Quarterly internal vulnerability scans must be performed by internal staff or a 3rd party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.

- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by the company's internal staff. The scan process should include re-scans until passing results are obtained.

20. Roles and Responsibilities

- Chief Security Officer (or equivalent) 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 business unit management personnel
- creating and distributing security incident response and escalation procedures that include:
- maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)

- The Information Technology Office (or equivalent) 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).

- System and Application Administrators shall:

- monitor and analyse security alerts and information and distribute to appropriate personnel
- administer user accounts and manage authentication
- monitor and control all access to data
- maintain a list of service providers
- ensure there is a process for engaging service providers including proper due diligence prior to engagement
- maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation

- The Human Resources Office (or equivalent) is responsible for tracking employee participation in the security awareness program, including:

- facilitating participation upon hire and at least annually
- ensuring that employees acknowledge in writing at least annually that they have read and understand the company's information security policy

- General Counsel (or equivalent) will ensure that for service providers with whom cardholder information is shared:

- written contracts require adherence to PCI-DSS by the service provider
- written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider

21. Transfer of sensitive Information Policy

- All third-party companies providing critical services to Conway Primary School must provide an agreed Service Level Agreement.

- All third-party companies providing hosting facilities must comply with the Company's Physical Security and Access Control Policy.

- All third-party companies that have access to Card Holder information must

    1. Adhere to the PCI DSS security requirements.

    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.

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

Keith Robertson/Karen Swannack/Kerisha Fariclough/Jagdeep Chana/Katrina Wright

Employee Name (printed)

School Office

Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the company 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 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 Information Security Policies, 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 company security 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 information security policies to the designated security officer.

_____

Employee Signature's

Appendix B

Asset/Device Name	Description	Owner/Approved User	Location
Ingenio ICT 250	Cardnet Machine	Conway/Lloyds	School Office

List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date
Lloyds Bank	0345 072 5555	Cardnet	Yes	06/07/16