Information Security Policy

Kids Photography Club (Admin Ltd)

_____

(Company Name)

11/10/2017_____

(Date)

Contents

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 fully understand this policy. 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 re-distributed to all employees and contractors where applicable.

Information Security Policy

Kids Photography Club Ltd handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

Kids Photography Club Ltd commits to respecting the privacy of all its customers and to protecting any customer data 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 and classification;
- Limit personal use of Kids Photography Club Ltd information and telecommunication systems and ensure it doesn't interfere with your job performance;
- Kids Photography Club Ltd 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.

1. Network Security

A high-level network diagram of the network is maintained and reviewed on a yearly basis. The network diagram provides a high level overview of the cardholder data environment (CDE), which at a minimum shows the connections in and out of the CDE. Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable should also be illustrated.

In addition, ASV should be performed and completed by a PCI SSC Approved Scanning Vendor, where applicable. Evidence of these scans should be maintained for a period of 18 months.

2. Acceptable Use Policy

Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Kids Photography Club Ltd established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions, either knowingly or unknowingly by individuals. Kids Photography Club Ltd 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 judgement regarding the reasonableness of personal use.
- Employees should take all necessary steps to prevent unauthorised access to confidential data which includes card holder data.
- Keep passwords secure and do not share accounts. Authorised 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.
- The List of Devices in Appendix B will be regularly updated when devices are modified, added or decommissioned. A stocktake of devices will be regularly performed and devices inspected to identify any potential tampering or substitution of devices.
- Users should be trained in the ability to identify any suspicious behaviour where any tampering or substitution may be performed. Any suspicious behaviour will be reported accordingly.
- 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 Kids Photography Club Ltd, 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.

3. Protect Stored Data

- All sensitive cardholder data stored and handled by Kids Photography Club Ltd and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is

no longer required by Kids Photography Club Ltd 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.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,

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.**

4. 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 Kids Photography Club Ltd 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 unauthorised disclosure.
- **Public data** is information that may be freely disseminated.

5. 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.

- Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.
- 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 C.
- Kids Photography Club Ltd 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.
- Kids Photography Club Ltd 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.

6. 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 Kids Photography Club Ltd sites. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device.
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces are 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 and=y 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. Kids Photography Club Ltd 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.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

7. 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 or by any other mode then it should be done after authorisation and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, etc.).
- 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.

8. Disposal of Stored Data

- All data must be securely disposed of when no longer required by Kids Photography Club Ltd, 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 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.
- Kids Photography Club Ltd 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.
- Kids Photography Club Ltd 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.

9. 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.

10. Credit Card (PCI) Security Incident Response Plan

- Kids Photography Club Ltd PCI Security Incident Response Team (PCI Response Team) is comprised of the Information Security Officer and Merchant Services. Kids Photography Club Ltd PCI security incident response plan is as follows:

    1. Each department must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
    2. That member of the team receiving the report will advise the PCI Response Team of the incident.
    3. The PCI Response Team 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. The PCI Response Team 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. The PCI Response Team 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.

  Kids Photography Club Ltd PCI Security Incident Response Team (or equivalent in your organisation):

  CIO
  Communications Director
  Compliance Officer
  Counsel
  Information Security Officer
  Collections & Merchant Services
  Risk Manager

  Information Security PCI Incident Response Procedures:

- A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform Kids Photography Club Ltd PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

Incident Response Notification

Escalation Members (or equivalent in your company):

Escalation – First Level:
Information Security Officer
Controller
Executive Project Director for Credit Collections and Merchant Services Legal Counsel
Risk Manager

Director of Kids Photography Club Ltd Communications

Escalation – Second Level:
Kids Photography Club Ltd President
Executive Cabinet
Internal Audit
Auxiliary members as needed

External Contacts (as needed)
Merchant Provider Card
Internet Service Provider (if applicable)
Internet Service Provider of Intruder (if applicable)
Communication Carriers (local and long distance) Business Partners
Insurance Carrier
External Response Team as applicable (CERT Coordination Centre 1, etc.) Law Enforcement Agencies as applicable inn local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network.
2. Gather, review and analyse the logs and related information from various central and local safeguards and security controls
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

How to notify Elavon in the event of an incident

1. **UK:**
   - E-mail: #ADCqueries-GB@elavon.com
   - Phone: 0 1923 651 622
2. **Ireland:**
   - E-mail: #ADCqueries-IE@elavon.com
   - Phone: 0402 25322
3. **Germany:**
   - #ADCqueries-DE@elavon.com
4. **Poland:**
   - #ADCqueries-PL@elavon.com
5. **Norway:**
   - #ADCqueries-NO@elavon.com
6. **Other Countries:**
   - #ADCqueries-EU@elavon.com

11. Transfer of Sensitive Information Policy

- All third-party companies providing critical services to Kids Photography Club Ltd 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 which 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 by a Payment Card industry representative, or a Payment Card industry approved third party.

12. User Access Management

- Access to Kids Photography Club Ltd is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorised by HR/line management.
- The job function of the user decides the level of access the employee has to cardholder data
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

    Name of person making request;
    Job title of the newcomers and workgroup;
    Start date;
    Services required (default services are: MS Outlook, MS Office and Internet access).

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all Kids Photography Club Ltd systems is provided by IT and can only be started after proper procedures are completed.

- As soon as an individual leaves Kids Photography Club Ltd employment, all his/her system logons must be immediately revoked.

- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

13. Access Control Policy

- Access Control systems are in place to protect the interests of all users of Kids Photography Club Ltd computer systems by providing a safe, secure and readily accessible environment in which to work.
- Kids Photography Club Ltd will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorisation provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to Kids Photography Club Ltd CISO.
- Access to Kids Photography Club Ltd IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any Kids Photography Club Ltd IT resources and services will be provided without prior authentication and authorisation of a user's Kids Photography Club Ltd Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by Kids Photography Club Ltd policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorisation by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.

- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

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

_____

Employee Name (printed)

_____

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

_____

Date

Appendix B – List of Devices

Asset/Device Name	Description	Owner/Approved User	Location

Appendix C - List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date