Data Security Policy

Contents

1. Introduction

1.1 Sri KDU International School, Subang Jaya ("**Sri KDU**") is committed to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

1.2 In this regard, the Personal Data Protection Act 2010 ("**PDPA**") imposes certain obligations upon Sri KDU in relation to the processing of personal data. These obligations are contained within seven (7) personal data protection principles.[1] The Security Principle relates to data security and requires us to take appropriate technical and organisational measures to safeguard personal data against such loss, misuse, modification, etc.

1.3 We recognise the importance of personal data to our business and the importance of privacy rights to individuals about whom we process personal data. This Policy is intended to assist our employees to comply with the requirements of the Security Principle. The term 'employee' is used in this Policy to include temporary and permanent employees, whether on permanent employment or contractual basis (but does not include an agent or sub-contractor of Sri KDU). This Policy may not be limited to protecting personal data but may also extend to all information which we hold.

1.4 The PDPA includes a number of defined terms which are used in this Policy. These terms are:

1.4.1 'Data Subject' means an individual (e.g. customer, employee, job applicant) about whom we process personal data and who is the subject of the personal data;

1.4.2 'personal data' means information in respect of commercial transactions that relates directly or indirectly to a Data Subject, who is identified or identifiable from that information or from that and other information in the possession of Sri KDU, including any sensitive personal data and expression of opinion about theData Subject;

1.4.3 'processing' means virtually anything we do with personal data such as collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, e.g. organisation, adaptation, alteration, use, disclosure, erasure or destruction;

1.4.4 'sensitive personal data' means personal data consisting of information as to the physical or mental health or condition of a Data Subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data that the Minister may determine by order published in the Gazette.

[1] Comprising: (i) General Principle, (ii) Notice and Choice Principle, (iii) Disclosure Principle, (iv) Security Principle, (v) Retention Principle, (vi) Data Integrity Principle, and (vii) Access Principle.

References to ‘we’, 'our' and ‘us’ refer to Sri KDU.

2. Your Responsibility

1.5 You must familiarise yourself with this Policy and implement its requirements within your department and working practices. Please refer to the Privacy Officer of Sri KDU for any clarification or guidance on this Policy orthe requirements of the PDPA in general.

1.6 Under the terms of your employment contract with Sri KDU**,** you have an obligation to comply with this Policy.

ANY FAILURE TO COMPLY WITH THIS POLICY MAY BE A DISCIPLINARY OFFENCE WHICH COULD RESULT IN DISCIPLINARY ACTION, OR IN MORE SERIOUS CASES, DISMISSAL. NEGLIGENT OR DELIBERATE BREACHES COULD RESULT IN CRIMINAL LIABILITY FOR YOU PERSONALLY.

3. Policy

1.7 The Security Principle requires Sri KDU, when processing personal data, to take practical technical and organisational steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

1.8 In order to assist us to comply with the Security Principle:

1.8.1 you must comply with the technical and organisational measures set out in the Annex to this Policy whenever you process personal data, as well as any other relevant information technology policy of Sri KDU as amended from time to time;

1.8.2 you must consider the nature of the personal data you are processing and determine whether the technical and/or organisational measures are commensurate to the harm that might result if there were a security breach. If the data are also confidential or sensitive personal data, an additional level of security will be required:

(a) Examples of confidential information may include HR data (e.g. employee records, payroll data); financial information (e.g. bank account and/or credit card details;

(b) Examples of sensitive personal data may include information about an individual's physical or mental health or condition, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data that the Minister may determine by order published in the Gazette;

1.8.3 you should only hold personal data for as long as it is required for the purpose for which those data were originally collected. Once the data are no longer required, you must destroy or delete those data securely;

1.8.4 you must immediately report all actual or suspected security breaches to the Relevant Department Privacy Officer. Where the breach involves personal data, you should also notify IT & Data Security Manager.

1.9 Sri KDU is responsible for taking reasonable steps to ensure the reliability of employees who have access to personal data. If you are responsible for the recruitment of employees (whether permanent, temporary or contract), you must assist us to comply with this requirement by:

1.9.1 screening/vetting all new employees;

1.9.2 ensuring all new employees sign terms and conditions which include confidentiality and security obligations;

1.9.3 taking up references for all new employees;

1.9.4 ensuring new employees are trained on the care and handling of personal data when they join (e.g. as part of their induction training).

1.10 As part of Sri KDU's obligation to ensure the reliability of employees who have access to personal data, we must provide training on the requirements of the PDPA. If you are responsible for training employees (whether permanent, temporary or contract), you must ensure that periodic training sessions (including refresher courses) are provided to employees on data protection topics, including the care and handling of personal data and security requirements.

1.11 Sri KDU is required to take additional security measures whenever it uses third parties to process personal data on its behalf. Third parties may include e.g. agency staff, IT contractors, providers of hosting services for our websites, outsourced service providers, payroll providers, computer maintenance providers, disaster recovery service providers. These third parties are referred to as 'data processors'. If you are responsible for the selection or appointment of any data processors, or are involved in contract negotiations with data processors:

1.11.1 you must make sure you only select data processors that provide sufficient guarantees in respect of the technical and organisational security measures they will use in relation to the processing of personal data. One of the ways in which you can achieve this is by carrying out suitability checks on the credentials of the data processors, as well as requiring all processors to enter into contracts with sufficient guarantees as to the technical and organisational security measures to ensure your compliance with the requirements of the PDPA;

1.11.2 you must enter into a contract in writing with each data processor. It is important to do this before the processing actually begins. If you are responsible for negotiating or drafting commercial contracts, please use one of our standard data processor contracts which includes a range of provisions designed to protect our personal data (when in doubt, please consult the Privacy Officer);

1.11.3 you must ensure that each processing contract makes it clear that data processors must only act on instructions from Sri KDU. We are responsible for the processing of all personal data, even if it is carried out on our behalf by a data processor. We must, therefore, maintain control over such processing at all times;

1.11.4 you must ensure that each data processor agrees to take appropriate technical and organisational measures to protect any personal data that it processes on our behalf from unauthorised or unlawful processing, accidental loss, destruction or damage. It is important that we specify any measures that must be taken;

1.11.5 you must ensure that we have the right to check the data processor's compliance with the terms of any processing contract. This may involve auditing the data processor from time to time to make sure that it is processing in accordance with our instructions and the security measures we have specified, as well as any other data protection related requirement of the PDPA, including the security standards set out under the Personal Data Protection Standards 2015 or any other guidelines, order and/or standards as set out by the Personal Data Protection Commissioner from time to time;

1.11.6 if the data processor will be holding personal data on our behalf and we do not also hold a copy of those data, we must make sure the processing contract includes a provision that requires the processor to assist us promptly with any data access/data correction request we might receive in relation to any of the personal data held by the data processor;

**A 'data access request' is a request received from a Data Subject asking for access to personal data which we process about him or her, whereas a 'data correction request' is a request received from a Data Subject asking to correct or update his/her personal data.*

1.11.7 you must ensure that upon termination of the processing contract, the processor promptly returns or destroys the personal data as directed by us;

1.11.8 if the data processor will be collecting personal data on our behalf, the processing contract must include an obligation upon the processor to give our privacy notice (which the processor is not allowed to modify) to all individuals about whom the processor collects personal data.

1.12 If the data processor proposes to use sub-processors to assist with the processing services, you should seek advice from the Privacy Officer as this will have consequences for Sri KDU and specific provisions will need to be included in the data processor agreement.

1.13 It is important to remember that just because we delegate some our processing activities to a data processor does not mean that we can delegate our legal responsibility to comply with the PDPA. As a data controller, we remain legally liable for the processing of personal data that are under our control, even if the processing activity itself was carried out by a data processor.

5. Contacts

1.14 If you have any queries about this Policy, please contact the Privacy Officer.

1.15 We reserve the right to change this Policy from time to time to take into account any relevant changes in law or guidance from the Personal Data Protection Commissioner. Changes made to this Policy will be notified through Sri KDU's internal communication channels OR posted on employees shared portals OR notified by memorandum OR by any other appropriate means.

[The remaining of this page has been intentionally left blank]

Annex

Technical and Organizational Measures

i) Technical Security Measures

For electronically processed personal data:

1 Prepare user IDs and passwords for employees who are authorised to access personal data

2 Terminate the user ID and password immediately when the authorised employee no longer handles Personal Data

3 Protection against malicious software/viruses/malware (e.g. software should not be installed from removable media or downloaded from the internet without virus checking it first)

4 Backing up data (e.g. daily back ups should be taken of all data on our systems; data should not be stored on local drives or exchangeable media as these will not be backed up)

5 Encryption

6 Secure exchange of information

7 User access controls (e.g. passwords should be allocated to all users; passwords should be changed on a regular basis; passwords should not be pinned up next to the computer or anywhere else where they could be seen; computers should have password activated screen savers that are turned on whenever the user is away from his or her desk; passwords should include a mixture of letters and numbers; avoid passwords that are easy to guess such as your name or date of birth; different access should be allocated to different users depending on job description and need to access personal or confidential data; different access rights should be allocated to individuals who have a need to modify personal or confidential data; read and write privileges should be allocated depending on job description and need)

8 Network access controls (including passwords)

9 Monitoring system access and use (including to maintain records of access to personal data periodically)

10 Guidance on mobile computing (e.g. do not leave laptops unattended in cars or in public places or on top of desks left unattended overnight)

11 Guidance on teleworking (e.g. do not use your home computer for work purposes unless you have cleared this with the IT department)

12 Transfer of personal data through mediums such as removable media devices and cloud computing services are not permitted without written authorisation from the top management of Sri KDU. If at all, any such transfer via such mediums or cloud computing services must be in compliance with the personal data protection principles in Malaysia, as well as those of other countries (where applicable)

13 Disaster recovery (e.g. ensure copies of personal data are stored off site in a secure and fire-proof location; business continuity plan should be created; disaster recovery and business continuity plans should be tested periodically)

14 Secure destruction or deletion of data and secure disposal of computer equipment and removable media (e.g. make sure that all hard drives are erased on all computers before their disposal)

15 Lockout mechanisms (e.g. system should automatically lockout when a user attempts to login using an incorrect password)

16 Security audits (e.g. check that networks comply with security policies; identify any risk areas)

17 User authentication

18 Anonymisation or pseudonymisation of data (e.g. for data processed for analytic purposes, these methods shall be considered, whichever is commercially viable).

For non-electronically processed personal data:

19 Ensure that personal data is stored in physical files in an orderly manner, and that such files are stored in a locked and safe area

20 Monitoring access and use (including to maintain records of access to personal data periodically)

21 Maintain records of transfer of personal data through conventional means such as post, service by hand, facsimile, etc

22 Secure destruction or deletion of data contained in documents or records (e.g. where you are destroying personal data or confidential information make sure that you do so securely by using a high specification shredder or confidential waste disposal agent)

ii) Organisational Security Measures

23 Maintain a register of all employees involved in the processing of personal data

24 Terminate employee's access to personal data or personal data systems after the employee's resignation, termination of employment, or where there is adjustment in accordance with changes in the organisation

25 control and limit the extent of employees' access to personal data or personal data systems for the purpose of the collection, processing and retention of personal data (e.g. for electronically processed personal data certain employees may only be allowed 'read-only' access to personal data, whereas other employees may be allowed to edit personal data, depending on the nature of the employee's position; for non-electronically processed personal data, only certain employees are allowed access to data storage area)

26 Entry controls to premises (e.g. visitors must sign in at reception and must be escorted around the premises at all times; visitors must wear identity badges at all times; you should approach anyone that you find walking around our premises that is not wearing a badge and ask them if you can assist them or alert security to their presence)

27 Secure access to computer facilities (e.g. keypads or locks on doors; authorised personnel allowed access only; install closed-circuit television cameras or provide 24-hour security, if necessary)

28 Positioning equipment so as to prevent screens from being overlooked (e.g. make sure that any personal data displayed on computer screens cannot be overlooked by passers-by)

29 Securing equipment when off-site

30 Secure disposal of equipment or its re-use/re-conditioning

31 Clear desk and clear screens policies to be implemented across the business

32 Observe confidentiality and security obligations in relation to personal data which you are handling

33 Procedure should be put in place to handle any breaches of security (e.g. policy should identify who is responsible for handling these breaches; audit trails should be available to show any unauthorised access; employees should be trained to report actual or suspected breaches immediately)

34 Training (e.g. on the care and handling of personal data; on security systems; on the procedure for handling security breaches; training records should be maintained for all employees; training should be refreshed periodically; employees should be contractually bound to attend all relevant training sessions; training can be delivered via the intranet or internet)

[The remaining of this page has been intentionally left blank]