ICT Acceptable Use Policy

Contents

Purpose

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Sri KDUInternational School, Subang Jaya:

- understand and follow procedures to ensure the safe and appropriate use of ICT at the service, including maintainingsecure storage of information
- take responsibility to protect and maintain privacy in accordance with Sri KDU Policy
- are aware that only those persons authorized by the Approved Provider are permitted to access ICT at Sri KDU International School, Subang Jaya understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.

Scope

This policy applies to Sri KDUInternational School, Subang Jaya. Throughout this document, all applicable partieshave been collectively referred to as “GIM Personnel”. This policy applies to all aspects of the use of ICT including:

- internet usage
- electronic mail (email)
- electronic bulletins/notice boards
- electronic discussion/news groups
- weblogs (blogs)
- social networking
- file transfer
- file storage (including the use of end point data storage devices –refer to Definitions)
- file sharing
- video conferencing
- streaming media
- instant messaging

Policy Statement

This policy provides a governing framework for secure and responsible use of Sri KDUInternational School, Subang Jaya provided computing devices, services and devices connected to Sri KDU Education networks. It is the responsibility of every Sri KDU personnel, to be aware of this policy and to conduct their activities in accordance to its recommendations

Actionable Items

Ownership and Return of Computing Devices

- Sri KDU International School, Subang Jaya provides computing devices to its staff. This is to support educational and work-related activities. Sri KDU provided devices shall continue to be the property of Sri KDU education, unless explicitly documented at the time of allocation;

- Upon completion of employment or the contractual term, personnel shall return all computing devices in their custody to the ICT department.

Protection of Sri KDU issued Computing Device

Sri KDU Personnel shall adopt reasonable measures to safeguard the Sri KDU issued equipment in their possession fromtheft and damage, including but not limited to the following:

- Computing devices shall not be left unattended in meeting rooms or at third-party locations including conferencesor hotel rooms;
- Computing devices shall not be checked-in as baggage during travel, unless mandated by the airport securitypersonnel;

Sri KDU personnel are not authorized to perform self-repairs. Faulty devices shall be handed over to the local ICT helpdesk for repairs and maintenance through authorized service vendors. Incidents related to lost, stolen or damagedcomputing devices shall be promptly reported to the ICT helpdesk.

NOTE:

- **On stolen / lost devices End-User is required to obtain a Police report**
- **Sri KDU ICT reserves the right to secure erase lost or stolen devices.**

Computing devices including portable storage devices, containing Sri KDu business information shall be handed over toICT helpdesk for disposal in a secure approved manner.

Acceptable Use of Computing Devices

Sri KDU issued computing devices shall be utilized in a manner that is consistent with organizational policies and withinthe confines of country laws and regulations. Sri KDU personnel shall not:

- Bypass organization or national security measures through fraudulent use of network protocol address i.e., use of private Virtual Private Networks or anonymity networks; *NOTE:* Sri KDU *personnel are permitted use of corporate Virtual Private Networks to connect to Sri KDU corporate network from remote locations.*
- Download, transmit, store or create in appropriate material as governed by the existing policies;
- Perform activities that would cause the network, website or applications to stop functioning or result in crashing,deletion, omission, destruction or cause fraudulent transaction i.e., activities classified as hacking or cracking;

- Install applications licensed as “free for non-commercial use”, shareware, adware and those not authorized and not licensed to Sri KDU Education;
- Provide remote or physical access to the computing device, to individuals other than designated ICT administrators;
- Reconfigure or tamper the computing device in any way that could result in failure, degraded performance or limited operations of software and implemented security controls i.e., Anti-Virus, Mobile Device Management, SCCM andother software agents;
- Interrupt installation of security patches and operating system upgrades on computing devices through forceful shutdown.
- Sri KDU personnel other than designated ICT staff, shall not hold privileged access / administrator rights on computing devices, to applications or to any other services hosted on Sri KDU networks.

- Sri KDU personnel shall not utilize allocated computing devices for testing new software / applications. Software testing shall be performed on designated test workstations installed on isolated networks. Contact ICT helpdesk fortest workstations.

Staff Passwords and User Accounts

Sri KDU provisions business tools and online subscriptions to its employees, which is controlled through a combination of user credentials (username and password). Sri KDU personnel shall exercise due care to prevent misuse of their allocated accounts. Sri KDU personnel:

- Shall not share their credentials (username password combination) with anyone. This includes colleagues,contractors, senior staff, managers or ICT staff;
- Shall not reveal or list passwords over emails, chats, questionnaires, sticky notes, security forms or other any othermedium;
- Shall change their password every 90 days and on their first logon;
- Shall not reuse passwords across personal and corporate accounts i.e., Utilize the same password across Facebook,google, Sri KDU corporate accounts and other portals;
- Shall not repeat the last four passwords;
- Shall choose passwords that are complex and difficult to guess. Passwords shall comply with the following attributes:
    - Shall not be guessable (include names, name of your pet, similar to the username, birthdates, or otherguessable parameters);
    - Shall not be composed of word or number patterns on the keyboard;
    - Password shall not be listed in hints on “Recover Password” questions;
    - Shall be at least eight characters in length and mandatorily include the following:
        - Include one upper case letter;
        - Include one number and;
        - Include one special character.
- shall be responsible for all activity that occurs, from use of their accounts and allocated computing devices.

Secure Use of Internet (within the school premises)

Internet access by Sri KDU personnel shall be consistent with their business need. Sri KDU personnel shall not utilize Internet access provisioned within Sri KDU premises to perform activities that could endanger Sri KDU Education’s reputation or classified as illegal as per national laws and regulations. Sri KDU personnel shall not utilize the Internet access provided in Sri KDU premises to:

- Commit fraud, forgery, harassment, intimidation or impersonation;
- Post or share derogatory, libelous or threatening messages or images against an individual, race, religion,organization or community;
- Download, upload or access inappropriate, extremist or terrorism related materials, pornographic content, maliciousssoftware (malware) and pirated copies of software or entertainment media;
- Use peer-to-peer or torrent based applications;

- Use anonymity networks (TOR, VPN) or access dark web;
- Perform activities that could cause corruption, disruption or result in unauthorized access of data on third-partywebsites or services on the Internet i.e., activities classified as hacking or cracking;
- Cause “Denial of Service” i.e., Use Internet services in a way that disrupts or blocks the service for others;
- Commit copyright infringement and provide third-parties, unauthorized access to Sri KDU network or to Sri KDU issuedcomputing devices through use of Virtual Private Networks.

Internet access within Sri KDU premises shall be limited to web portals only. Access to Internet hosted services over non- standard protocols such as FTP, POP3, IMAP, RDP is not permitted. Connecting to free public Wi-Fi hotspots for Internet access (cafés, hotel lobbies, airports) utilizing Sri KDU issued devices is not recommended. Personal use of Internet within Sri KDU premises during business hours should be minimal and must not affect the individual’s ability to perform their assigned responsibilities.

Secure Use of Electronic Communication

Sri KDU personnel should use their business email account with due care to avoid misuse. Sri KDU personnel shall not:

- Use Sri KDU business email address to subscribe to mailing lists, external services not related to business;
- Utilize named Sri KDU email accounts (allocated corporate email accounts) for promotional messages oradvertisements;
- Share executable programs or scripts to internal or external recipients over email;
- Generate or forward chain mails containing derogatory, libelous or threatening messages, images against anindividual, race, religion, organization or community;
- Remove or modify the system generated disclaimer notice and email signatures;
- Auto-forward Sri KDU corporate emails to external addresses / domains or personal accounts;
- Utilize alternate modes to communicate Sri KDU business information such as messenger services or email servicesnot provisioned by Sri KDU;

Sri KDU personnel shall exercise caution in responding to requests soliciting user credentials for Sri KDU accounts thatclaim to come from ICT department or service providers over email or telephone calls.

NOTE: Under any circumstances, Sri KDU ICT or any service provider will not request validation of Sri KDU user accounts or user credentials (username / password) over an email, URL, SMS or a telephone calls. All such requests should be promptly notified to ICT helpdesk and should not be complied with.

Sri KDU personnel are not permitted to utilize corporate email for personal correspondence; *NOTE: Sri KDU Education reserves the right to monitor and disclose Sri KDU provisioned email communications for legal purposes without prior notice. All email correspondence performed using Sri KDU corporate email accounts shall remain the property of Sri KDU Education and is considered official data.*

Secure Sharing and Storage of Data

Sri KDU personnel shall exercise due care in handling Sri KDU business data in their custody. Sri KDU personnel are not authorized to copy or move Sri KDU business data:

- To personal storage, personal cloud storage or personal computing devices;
- To third-party online portals or cloud applications. Unless the third-party / service provider / vendor is contractuallyengaged with Sri KDU and contractually obligated to safeguard Sri KDU business data in the cloud (service provider’s
  / vendors environment);

Sri KDU personnel shall not share Sri KDU business data through unauthorized channels, i.e., personal email, messengerservices, free to use data sharing and cloud storage platforms; e.g. Gmail, Yahoo mail, WhatsApp, Dropbox, WeTransfer, personal cloud storage accounts among others.

NOTE: Sri KDU reserves the right to restrict access to cloud storage platforms within its premises.

Sri KDU personnel are not permitted to configure data shares on their local computing devices. Sri KDU personnel shall only utilize Sri KDU issued Corporate Microsoft OneDrive cloud account or the Sri KDU school provisioned platform, to share data with relevant external business parties;

- Data shares shall be configured only after relevant approvals from data owners / Head of the Department;
- Access to data shares shall be, explicitly restricted to designated individuals of intended business parties anddisabled within 15 days of activation;

NOTE: Prior to transfer of data, Sri KDU personnel shall ensure the recipient organization has legally entered intoa confidentiality agreement with Sri KDU Education, is made aware of the sensitivity of the data, shall maintain its confidentiality and also limit the use of data shared for designated purpose only.

Sri KDU personnel are permitted to utilize approved storage location / platforms for storing business data. List of approved storage locations / platforms include:

- Sri KDU internal file-shares accessible from Sri KDU network only
- School provisioned internal file-shares accessible using Sri KDU issued computing devices;
- Sri KDU issued "OneDrive" accounts accessible using Sri KDU credentials or Cloud storage service provisioned byrespective schools where Microsoft OneDrive is not utilized;
- Local storage on Sri KDU issued computing

devices;Backups

In order to ensure continuity of operations, Sri KDU personnel are responsible to backup all business data on theircomputing devices;

- Sri KDU personnel shall regularly backup their locally generated data to Sri KDU provided Cloud drive (Sri KDU issuedCorporate Microsoft OneDrive account);
- Under any circumstances SRI KDU personnel shall not backup files / data containing SRI KDU business data to personalstorage (including Portable storage drives i.e. USB Hard Drives or Pen Drives or personal cloud storage accounts).

NOTE: Refer OneDrive tutorials online on guidance to use OneDrive or contact your local ICT helpdesk foradditional support.

BYOD (Bring Your Own Devices) for official use

Sri KDU personnel are permitted to register one personal handheld device (Tablet computer or Mobile Phone) for Sri KDU official use under BYOD program;

Personal devices shall mandatorily comply with the following standards in order to be eligible for registration under BYOD program;

- Devices should be running a supported platform:

- Android
- IOS
- Devices should be covered by the manufacturer for security updates and host asupported version of the OperatingSystem or an updated firmware;
- Devices should not be configured with privileged access i.e., jailbroken or rooted devices are not permitted to beregistered;
- Device hardware or software should not be tampered with, infected with malware or have applications fromunauthorized app-stores installed;

NOTE:

- ***Sri KDU ICT reserves the right to withdraw a BYOD registered device or discontinue support to a specificplatform if it is considered a security threat.***
- ***Supported platforms and versions are subject to change depending on evolving technology landscape.Contact ICT helpdesk for supported versions.***

Personal devices registered under BYOD shall be mandatorily enrolled in MDM (Mobile Device Management) solutionapproved and deployed by SRI KDU ICT and utilize approved applications to ensure secure access and storage of Sri KDU business data;

- Sri KDU personnel shall not modify, tamper, disable or uninstall the Mobile Device Management software and thesecurity policies deployed on the BYOD registered personal devices;
- Sri KDU personnel are responsible for the security updates, care maintenance and backup of the personal deviceregistered under BYOD;
- Sri KDU personnel shall promptly inform ICT Helpdesk for a temporary withdrawal from BYOD program, beforehanding the devices to external agencies for repairs / maintenance or disposal;
- Lost or stolen devices shall be reported within 8 hours to the ICT helpdesk by the device owners;

NOTE: Sri KDU ICT reserves the right to secure erase lost or stolen device registered under BYOD program.SRI KDU Education will not be responsible for compensation or recovery of lost personal data on the device.

Sri KDU Education owns the right to all Sri KDU business data stored on personal devices; *NOTE: Contact your local ICTadministrator to register your Personal device under BYOD program.*

<u>Remote Support and Access to Third Parties</u>

Sri KDU personnel are not authorized to subscribe to third-party support for troubleshooting or management ofapplications and computing devices in SRI KDU network:

- Support and maintenance that requires third-party access to Sri KDU network or computing devices shall be loggedand managed through ICT helpdesk;
- Sri KDU authorized ICT personnel shall monitor access by third-parties to the Sri KDU network or devices connectedto Sri KDU networks;
- Provisioning access without supervision to third-parties for computing devices that are connected to Sri KDU network is prohibited;
- Sri KDU personnel shall not utilize unregistered or unlicensed software for remote access.

<u>Incident Reporting</u>

Sri KDU personnel shall report all incidents to enable implementation of appropriate corrective actions. Sri KDU personnelshould promptly report any of the following incidents to ICT helpdesk;

- Loss of Sri KDU business data through:
- Lost / stolen Sri KDU provided computing device;
- Loss of personal device registered under BYOD;

- Lost storage device containing Sri KDU business data;
- Compromised credentials for Sri KDU corporate accounts under the individuals' care;
- Suspicious system behavior;
- Suspicious emails sent from Sri KDU account under the individuals' care;
- Suspected malware;
- System misconfiguration or opportunities to circumvent implemented system controls discovered during the courseof daily business operations;
- Suspicious devices attached to systems or network points;
- Suspicious / look-alike wireless networks visible in Sri KDU premises;
- Any identified violation of this

policy;Right to Change

Sri KDU, reserves the right to modify or amend this policy in accordance to applicable laws, regulations and corporatepolicies.

SRI KDU , reserves the right to monitor and

- Review the use of SRI KDU network and SRI KDU provided computing devices;
- Remove / uninstall applications, tools or data / content on SRI KDU provided computing devices that is in violation ofSRI KDU policies and national laws;
- Block network access to devices and user accounts:
- That are compromised;
- That do not comply with SRI KDU policies or considered a security threat to SRI KDU network;
- Implement appropriate technology and tools on SRI KDU owned computing devices and networks to ensurecompliance to SRI KDU policies;
- The tool agents include but not limited to: Mobile Device Management, Firewall, Anti-Virus, F uture Digital agentsand others.

Device allocation to staff\student

- Administrative staff – All admin staff entitled for DELL Laptop or DELL Desktop
- Secondary teaching staff – All secondary teaching staff is entitled for DELL laptop
- Primary teaching staff - All primary teaching staff is entitled for DELL laptop and iPad
- Teaching assistant - All teaching assistant are entitled for DELL laptop
- Students – All GIM students is enroll in BYOD programme.

Supporting Documents

- Security Policy
- Registers of records to be obtained
- New hire IT form
- New joiners technology guide
- IT service desk application user guide

Responsibility

All staff at SRI KDU International School, Tropicana Metropark, including permanent staff, management, volunteers, consultants, officers and temporary staff, are responsible for complying with this Policy. Any breach of this Policy couldpotentially result in disciplinary action.

Promulgation and Implementation

This Policy & Procedure will communicated though out the School Community in the form of:

- Distribution of e-mails to ICT helpdesk, Reprographics' School Principal / School staff / CEO and Regional Risk &Compliance department.