Appendix I

Proposed IT Policy

KOLEJ DAMANSARA UTAMA SDN BHD

CORPORATE

IT POLICY GUIDELINE

Outsourcing

1. KDU
   1.1. Determine KDU's core competencies. It is important to determine the skill sets that must be retained for the future of the business.
   1.2. It is imperative that core technologies be insourced / kept in-house, or cosourced.
   1.3. Identify at least TWO (2) staff to manage the outsourcing contract. One of these must be a senior executive with experience in administering leasing or licensing arrangements, be IT-literate and have good relationship management.
   1.4. Draw up a list of requirements that includes the following:
      1.4.1. performance expectations
      1.4.2. measurement methods for response time
      1.4.3. transaction volumes
      1.4.4. security / access control
      1.4.5. disaster recovery / backup in the event of a catastrophe
      1.4.6. processing requirements of the new applications
      1.4.7. degree of distributed processing among LAN nodes
      1.4.8. complete applications system documentation
   1.5. Maintain short-term contracts not exceeding 2 years
2. Outsourcing Vendor
   2.1. Must understand KDU's business and work with KDU as a partner.
   2.2. Must be familiar with the education industry's regulations and its critical success factors.
   2.3. Agreements must be adapted to meet KDU's changing needs.
   2.4. Must provide a list of the existing customers

Leasing

1. Lease that which depreciates.
2. Lease only for the Computer Centre teaching laboratories.

3. Keep the leasing period to within two years.
4. Maintain a leasing interest rate of approximately 6.5%.

Purchasing

1. Purchase from as few sources as possible.
2. Avoid new or early releases of products and services.
   2.1. Technical support from the vendor may still be deficient. Their staff may still be familiarising themselves with the product's features.
3. Avoid trailing edge products.
   3.1. These are seldom feasible as support is limited.
   3.2. Staff will also be reluctant to use them.
   3.3. Maintenance costs are higher.
4. Purchase Academic Editions (AE) of commercial software. Opt for license packs whenever possible. These tend to provide greater savings per unit as the number of licenses purchased increases.
5. Maintain anti-virus software on subscription-based licensing. This will ensure regular, e.g. quarterly, updates.
6. Install a software license metering package to monitor and manage the software licenses.
7. Ensure that the vendor provides good after-sales service support.
8. If necessary, insist on the list of the vendor's customers.

Cascading

1. This practice may be used to stretch IT budgets.
2. However, user requirements, current equipment and planned upgrades must be tracked **before** computer equipment are re-deployed to lower-end users.
3. Generally, a cascade strategy that is limited to ONE re-deployment during the equipment's lifetime can contribute positively to KDU's equipment

productivity.

Hardware Component Upgrades

1. Generally, RAM, or computer memory are economically justifiable and can extend the life of computer equipment.
2. However, note the following:
   2.1. Equipment targeted for upgrade are likely to be aging systems that are out of warranty. As such the residual value is not increased very much. Their only real value will be as spare parts.
   2.2. More administrative costs will surface from identifying upgrade candidates, managing and tracking warranties on upgrade components and maintaining additional supplier relationships.
   2.3. It is highly unlikely that such upgraded systems will be able to exploit new technologies.
3. KDU must look beyond capital expenditures when evaluating component upgrades.

Internet and Email

1. KDU encourages the use of the Internet and email because they make communication more efficient and effective.
   1.1. Their purpose is to facilitate college business.
   1.2. Every staff member has a responsibility to maintain and enhance the college's public image and to use the college email and to access to the Internet in a productive manner.
2. The college email and Internet access may not be used for transmitting, retrieving or storage of any communications of a discriminatory nature or pornographic materials. There must be no transmission of messages with derogatory or inflammatory remarks about an individual's
   2.1. Race

2.2. Age
2.3. Disability
2.4. Religion
2.5. National origin
2.6. Physical attributes
2.7. Sexual preference

3. Electronic media may also not be used for any other purpose that is illegal or against college policy or contrary to the college's best interest. Solicitation of non-college business or any use of the college email or Internet for personal gain is prohibited.

Communications

1. Each employee is responsible for the content of all text, audio or images that they place or send over the college's email/Internet system.
   1.1. No email or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else or someone from another college.
   1.2. All messages communicated on the college's email/Internet system should contain the employee's name.
2. All communications sent by employees via the college's email/Internet system must comply with this and other college policies and may not disclose any confidential or proprietary college information.
3. Staff may not indulge in Internet chatting during office hours of between 9am – 5pm. This is allowed only after 5pm.

Copyright of Content

1. Copyrighted materials not belonging to KDU, may not be transmitted by employees on the college's email/Internet system.
   1.1. Employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission, or as a single copy to reference only.

2. Failure to observe copyright or license agreements may result in disciplinary action up to and including termination.

Software

1. To prevent computer viruses from being transmitted through the college's e-mail/Internet system, there will be no unauthorised downloading of any unauthorised software.
2. Any software downloaded must be registered with the college IS Department. Employees should contact the IS Department if they have any questions.

Security

1. The college routinely monitors usage patterns for its email/Internet communications. The reasons for this monitoring are many, including cost analysis/allocation and the management of the college's gateway to the Internet.
2. All messages created, sent, or retrieved over the college's email/Internet are the property of the college and should be considered public information. The college reserves the right to access and monitor all messages and files on the college's email/Internet system.
3. Employees should not assume electronic communications are totally private and should transmit highly confidential data in other ways.

Violations

1. Any employee who abuses the privilege of college facilitated access to email or the Internet, will be subject to corrective action up to and including termination.
2. If necessary, the college also reserves the right to advise appropriate legal officials of any illegal violations.

be backed up or archived, in such a way that the data can be recovered if the workstation file system is destroyed.

2. Daily backups of the centrally stored corporate data must be effected without exception.
3. Two kinds of backup media are available,
   3.1. Tapes. These have capacities up to 24 GB with data compression software.
   3.2. Removable disks. These have capacities of 100MB-1GB. JAZZ or ZIP drives look like thicker floppy disks but still require a special drive/hardware to operate them.
4. Networked file storage includes the following:
   4.1. Workstations using some form of networked file system can place important files upon the local server.
   4.2. However, there is a limit to how much data can be stored this way as servers have space restrictions.
5. File management
   5.1. Only work files require backing up.
   5.2. All work files, e.g. word-processor documents, spreadsheet files and database files, should be saved into an area separate from the respective applications. This will greatly simplify backing them up.
   5.3. In the event of a major workstation system failure, applications can be restored from disk or CD-ROM. The data then can be restored from the backup device.

Disaster Recovery

1. A minimum of two (2) copies of the complete applications system documentation must be available. One of these copies should be kept in a secured off-site location, e.g. safe deposit box in a bank.
2. The backed up media must be stored in the KDU safe awaiting Next Business Day (NBD) transfer to a secured off-site location, e.g. safe deposit box in a bank.
3. Enter into a maintenance agreement with its hardware suppliers so as to effect a quick replacement of the damaged hardware.

IT Staffing

1. Ensure that the IT equipment and infrastructure are upgraded on an annual basis so as to project a dynamic college which would attract equally dynamic and talented staff.
2. Adopt industry-standard certification training programmes to motivate and retain staff.
3. Draw up a long-term self-evaluation programme for the staff. The pertinent areas should include the following:
   3.1. Current duties
   3.2. Significant achievements during the evaluation period, e.g. the current year
   3.3. Self-defined targets for the next evaluation period, e.g. the next year
   3.4. Resources and opportunities that must be provided by the employer to achieve the self-defined targets

Communication of Policy

Communicate this policy in several ways, including:

1. Online message that appears when the user logs onto the computer network.
2. Short policy statement in the employee handbook.
3. Orientation and hiring statement notifying new employees of the IT policy.
4. Run training sessions where policies are explained in detail can go a long way in allaying anxieties regarding the computer / network/ Internet / email usage.

EMPLOYEE AGREEMENT

BETWEEN

KOLEJ DAMANSARA UTAMA SDN BHD

AND

<EMPLOYEE>

DATED DAY OF 1999

Corporate Email and Internet User Agreement

This Employee Agreement is between Kolej Damansara Utama Sdn Bhd, henceforth known as "KDU", and _____

I have received a copy of KDU's Corporate IT Policy Guideline on email/Internet usage, policy #____, dated, _____. I recognise and understand that the company's email/Internet systems are to be used for conducting the company's business only. I understand that use of this equipment for private purposes is strictly prohibited.

I have read this document and agree to follow all policies and procedures that are set forth therein. I further agree to abide by the standards set in the document for the duration of my employment with KDU.

I am aware that violations of this corporate guideline on email/Internet usage may subject me to disciplinary action, up to and including discharge from employment.

I further understand that my communications on the Internet and email reflect KDU world wide to our competitors, customers and suppliers. Furthermore, I understand that this document can be amended at any time.

_____ _____

Employee Signature **Date**

_____

Employee Printed Name

_____ _____

KDU Representative Signature **Date**

_____

KDU Representative Printed Name

KDU Privacy Statement

Disclaimer

KDU will not obtain personally-identifying information about you when you visit our site, unless you affirmatively choose to provide such information to us.

When you visit our site, we automatically collect and store only the following information about you, which does not contain personally identifiable information:

Your hostname or IP address
The domain from which you access our site
The day, month and year you access our site

We use this information to measure the number of visitors to the different sections of our site, and to make our site more useful to future visitors. We do not sell or transfer to third parties any of information that we collect from every applicant.

If you identify yourself by sending an email, posting information, or submitting a form via the KDU homepage, you also may decide to include personally-identifying information in that communication for example, when requesting information or registering in the on-line KDU Application Form.

If you choose to submit personally-identifying information, we may use this information for marketing. This information is stored by KDU and will be used solely for KDU's marketing purposes.