ASPECT 2: TECHNICAL SECURITY

POLICY STATEMENTS

- ✓ The IES will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:
- ✓ School technical systems will be managed in ways that ensure that the school meets recommended technical requirements there will be regular reviews and audits of the safety and security of school technical systems.
- ✓ Servers, wireless systems and cabling must be securely located and physical access restricted appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- ✓ Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff external agency CADD Emirates.
- ✓ All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.
- ✓ Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- ✓ Mrs. Sangeetha is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- ✓ Mobile device security and management procedures are in place (students and staff are restricted on use of mobile)
- ✓ School management service provider/ technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. (Schools may wish to add details of the monitoring programs that are used)
- ✓ Remote management tools are used by staff to control workstations and view users' activity
- ✓ An appropriate system is in place (online log book) for users to report any actual/potential technical incident to the online safety coordinator /network manager/technician
- ✓ An agreed policy is in place (to be described) regarding the downloading of executable files and the installation of programs on school devices by users

- ✓ An agreed policy is in place (to be described) regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.
- ✓ An agreed policy is in place regarding the use of removable media (e.g.memory,usb,sticks/CDs/DVDs)by users on school devices (see school personal data policy template in the appendix for further detail)
- ✓ The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms ,trojans etc.
- ✓ Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.(see school personal data policy template in the appendix for further detail)

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- ✓ Users can only access data to which they have right of access
- ✓ No user should be able to access another's files(other than that allowed for monitoring purposes within the school's policies)
- ✓ Access to personal data is securely controlled in line with the schools personal data policy
- ✓ Logs are maintained of access by users and of their actions while users of the system
- ✓ There is effective guidance and training for users
- ✓ There are regular reviews and audits of the safety and security of school computer systems
- ✓ There is oversight from senior leaders and these have impact on policy and practice.

Members of staff will be made aware of the school password policy:

- ✓ At inductuon
- ✓ Through the school online safety policy and password security policy
- ✓ Through the acceptable use agreement

Students/pupils will be made aware of the school's password policy:

- ✓ In lessons
- ✓ Through the acceptable use agreement

Audit/monitoring/reporting/review:

- ✓ The responsible person (mrs. Sangeeta and mr.khaleel)will ensure that full reccords are kept of:
- ✓ User ids and requests for password changes
- ✓ User logons
- ✓ Security incidents related to this policy

Cyber- attack come in many shapes and sizes, oor the vast majority are quite straightforward in nature and carried out by relatively unskilled individuals: the digital equivalent of a thief trying your front door to see if it is unlockd. The device is designed to prevent these attacks and explains in more detail five fundamental steps to making your organization more secure:

- ✓ Use a firewall to secure your internet connection
- ✓ Choose the most secure settings for your devices and software

- ✓ Control who has access to your data and services
- ✓ Protect yourself from viruses and other malware
- ✓ Keep your devices and software up to date.

Contact

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to info@iesrak.com

For any other queries, please contact us on: info@iesrak.com