IT Policy

Introduction

IT Policy in Education is much more than the mere collection and distribution of knowledge. It offers intellectual hospitality, opportunities for innovation, creativity; power of thought and imagination. It envisages development of character and inculcation of a firmness of mind and zeal to offer one's best to the world. Education is the means of unfolding moral and spiritual potentialities of individual.

Scope of IT policy

› Rules for access to administrative data, including definitions explaining what it is and the rules for using it. Employees who access administrative data must use it according to the rules or risk disciplinary consequences.

› States the codes of practice with which the organization aligns its information technology security program to safeguard the institution‟s computing assets in the face of growing security threats. This significant challenge requires a strong, persistent and coordinated program that leverages widely accepted, effective security practices appropriate for the higher education environment.

› Strictly limits the circumstances under which highly sensitive data may be stored on individual-use devices and media. It further mandates that strict security requirements be met when highly sensitive data must unavoidably be stored on individual- use electronic devices or electronic media.

› The Organizational Web pages must not be used for commercial purposes.

› Explains the conditions under which third parties (e.g., auditors, consultants) are allowed direct access to the network.

› Explains all users‟ responsibilities for maintaining the security of their devices on the organizations network.

› Explains rules for maintaining privacy, confidentiality, and integrity of the computing environment while using resources appropriately Defines ban (and exemptions) on employee access to obscene materials & sexually explicit material via state equipment. Rules for using shared computing resources such as public labs.

Aims of IT Policy

PJLCP Information Security Policies are necessary to ensure that important data, Institution plans and other confidential information are protected from theft or unauthorized disclosure. If employees of any organization are not aware of these policies, they will not know what is expected of them when they handle such confidential information.

› Empowering students and teachers by enabling online teamwork for increased participation, collaboration and information sharing through the use of email, the Web and other remote collaboration tools.

› Enabling the rapid creation and inexpensive distribution of educational information and knowledge.

› Encouraging professional development, in service training, remote support and mentoring for

lifelong learning for teachers and students.

› Facilitating fast and easy access to information and expertise around the world.

› Increasing motivation through the use of multimedia (sound, video, graphics, animation and text.)

› Allowing each student to learn at his/her level and speed thereby giving pupil‟s greater control over their own learning.

› Enhancing the development of the abilities of mentally and physically challenged students.

› Promoting active rather than passive learning.

› Engaging students in research, data analysis and problem solving, thereby facilitating higher-order thinking processes such as synthesizing, interpreting and hypothesizing.

Policy Statement

"It shall be the responsibility of the Institution to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorized members of staff, and to ensure the integrity of all data and configuration controls."

Benefits of Information Technology

› Information Technology can affect in the spread of education and to enable greater access to it. IT increases flexibility so that students can access educational resources regardless of time and geographical barriers. They can affect the way that students are given instruction and how they learn. They enable collaborative development of skills and abilities to create knowledge. This as a result will bring a better preparation for students, lifelong learning and the opportunity to join industry.

› Increase access, Flexibility of content and distribution Combination of education and work the methods are focused on the student.

› High quality, cost-effective professional development in place of labor. Improve the skills of employees, increase of productivity. Developing a new culture of learning. Sharing of costs and timing of training among employees.

› Increased capacity and cost effectiveness of the system education. Achievement of target groups that have limited access to traditional education. Support and improve the quality and relevance of existing structures of education. Provide links to education institutions and curricula with the networks.

› IT can also help improve the performance of knowledge workers and enhance organizational learning. Externally, it can improve the performance of knowledge workers in customer, supplier and partner organizations; add information value to existing products and services; create new information-based products and services.

› In terms of Functionality and Flexibility, internally IT can help improve infrastructure performance thus increasing functionality and the range of options that can be pursued. Externally, it can help create an efficient, flexible online/offline platform for doing coordination with educational Organizations.

Limitations of IT use in Education

› IT as a modern technology that simplifies and facilitates human activities is not only Advantageous in many respects, but also has many limitations. Many people from inside and outside the education system, think of IT as "Panacea" or the most important solution to institution problems and improvements. However, many conditions can be considered as limitations of IT use in education. The limitations can be categorized as teacher related, student related, and technology related. All of them potentially limit the benefits of IT to education.

› The other limitation of IT use in education is technology related. The high cost of the technology and maintenance of the facilities, high cost of spare parts, virus attack of software and the computer, interruptions of internet connections, and poor supply of electric power are among the technology related limitations of IT use in education.

Summary of Main Security Policies

› Confidentiality of all data is to be maintained through discretionary and mandatory access controls, and wherever possible these access controls should meet with security functionality.

› Internet and other external service access are restricted to authorized personnel only.

› Access to data on all laptop computers is to be secured through encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.

› Only authorized and licensed software may be installed, and installation may only be performed by Department staff.

› The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it will be removed from the workstation immediately.

› All diskette drives and removable media from external sources must be virus checked before they are used within the Organization.

› Passwords must consist of a mixture of at least 4 alphanumeric characters, and must be changed every 30 days and must be unique.

› Workstation configurations may only be changed by Department staff.

› The physical security of computer equipment will conform to recognized loss prevention guidelines.

› To prevent the loss of availability of I.T. resources measures must be taken to backup data, applications and the configurations of all workstations.

Virus Protection

› The Department will have available up to date virus scanning software for the scanning and removal of suspected viruses.

› Corporate file-servers will be protected with virus scanningsoftware.

› All workstation and server anti-virus software will be regularly updated with the latest anti-virus patches by the Department.

› No disk that is brought in from outside the Organization is to be used until it has been scanned.

› All systems will be built from original, clean master copies whose write protection has always been in place. Only original master copies will be used until virus scanning has taken place.

› All removable media containing executable software (software with .EXE and .COM extensions) will be write protected wherever possible.
› All demonstrations by vendors will be run on their machines and not the Organizations.
› Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.
› New commercial software will be scanned before it is installed as it occasionally contains viruses.
› All removable media brought in to the Organization by field engineers or support personnel will be scanned by the Department before they are used on site.
› To enable data to be recovered in the event of virus outbreak regular backups will be taken by the Department.
› Management strongly endorses the Organizations‟ anti-virus policies and will make the necessary resources available to implement them.
› Users will be kept informed of current procedures and policies.
› Users will be notified of virus incidents.
› Employees will be accountable for any breaches of the Organizations‟ anti-virus policies.
› Anti-virus policies and procedures will be reviewed regularly.
› In the event of a possible virus infection the user must inform the I.T. Department immediately. The I.T. Department will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

Access Control

› Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
› Users requiring access to systems must make a written application on the forms
› Where possible no one person will have full rights to any system. The I.T. Department will control network/server passwords and system passwords will be assigned by the system administrator in the end-user department.
› The system administrator will be responsible for the maintaining the data integrity of the end-user departments data and for determining end-user access rights.
› Access to the network/servers and systems will be by individual username and password, or by smartcard and PIN number/biometric.
› Usernames and passwords must not be shared by users.
› Usernames and passwords should not be written down.
› Usernames will consist of initials and surname.
› All users will have an alphanumeric password of at least 4 characters.
› Passwords will expire every 30 days and must be unique.
› Intruder detection will be implemented where possible. The user account will be locked after 5 incorrect attempts.
› The department will be notified of all employees leaving the Organizations employment. The Department will then remove the employee's rights to all systems.
› Network/server supervisor passwords and system supervisor passwords will be stored in a secure

location in case of an emergency or disaster, for example a fire safe in the Department.

› Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.

› Default passwords on systems such as Oracle and SQL Server will be changed after installation.

› Access to the network/servers will be restricted to normal working hours. Users requiring access outside normal working hours must request such access in writing on the forms provided by the Department.

› File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and Files scan rights to directories, files will be flagged as read only to prevent accidental deletion.

DINESH RAMKRUSHNA RAO CHAPLE

Digitally signed by DINESH RAMKRUSHNA RAO CHAPLE
Date: 2023.12.23 15:42:42 +05'30'