Managing IT Resourses in Educational Institute

The Situation

Whether we like it or not, computers and the Internet have become a part of our life and are now widely used at school, libraries, homes, work,...

Internet access to students is becoming an essential part of the learning environment. In addition, it also brings the serious problem of inappropriate content on the Internet.

The Internet is like a vast playground, with a lot of potential for fun and enrichment, but also potential for problems. It is important to remember that some types of online trouble are more serious.

According to a study by the Kaiser Family Foundation, 70 percent of teens have accidentally stumbled across pornography online.

Given the diversity of the information carried on the Internet, student access to inappropriate material is a major concern of many parents and teachers.

Academic Institutes are also concerned about the availability of violent content.

In an educational environment where all the desktops are equipped with free and easy access to the Internet, it can be very difficult for teachers to keep the students focused on the lesson without any control.

It is important to balance the students need to utilize the technology to its full potential for academic purpose and misuse.

One could then argue that there is a real need to monitor how students use the Internet.... For example,

- As a faculty or teacher,
- Do we know what web sites students access?
- Do we know if students are chatting online, downloading files,... when they should be doing their coursework?
- Do we know what web sites student's friend exposes him/her to when they surf the Internet together?
- Do we know whether student has been doing his/her coursework or playing Games?
- Do we know who is using most of the computer & Internet time for non-academic purpose when someone really needs for submitting assignments and research Paper?
- Do we know how to avoid abuse of campus computers and block illegal use? And so on...

For these reasons, rather than advocating policies that completely block students in regard to the content of their web sites, it is better to restrict the access timings, sites and contents.

Cyberoam Solution

A basic approach could be:

- Identify what you are trying to protect
- Look at whom you are trying to protect it from
- Identify potential risks
- Define policies - Policies should be such that it takes the appropriate disciplinary action to encourage students/staff to use resources to do the right thing
- Consider monitoring continually in order to be up to date with the latest weaknesses

Policies outline how students can use the technology, what they cannot do with it and the consequences of violating the policy.

Most Academic Institutes see some level of personal Internet use as a way to support their Students' growth, rather than undermine it, and have relatively liberal policies about the usage

Cyberoam helps you achieve the above goals by defining quota and various policies like Internet access policy, Surfing quota policy, Security policy and Printing policy.

Cyberoam can:
- Completely block Internet
- Allow access only to the specified Web sites
- Deny access to any specified domain
- Restrict inappropriate surfing, and schedule Internet ON at only certain times of day
- E-mail, FTP sites, Instant Messaging and Newsgroups can also be restricted

Surfing Quota

Academic Institutes can manage Internet access for students by means of the surfing Quota. Allocate surfing quota to each student based on the student's academic load and which covers course-related Internet access.

Staff Internet access can also be managed by the means of surfing quota. Allocate surfing quota to staff based on the requirement.

Cyberoam Benefits

> Limit or Block the Internet usage to the specified times of day and if required to the specified sites also
>
> Have Control on Internet and Messaging activity
>
> Block any sites that you do not wish your students to view
>
> Restrict non-educational surfing activity
>
> Reduce strain on network bandwidth resources
> Reduce legal liability
>
> Control, Limit, block access to E-mail, Chat sites, Newsgroups

Institutes can think in terms of charging students and staff for the Internet used over and above the quota allocated. This will promote the responsible use of Internet access and Institutes can generate some additional funds for re-allocation to technology upgrades.

Students and Staff should be aware to the fact that the use of Internet over and above the allocated quota is not free and will be charged.

Printing Quota
Similar to the surfing quota, printing quota i.e. limit to number of pages printed, can be allocated to minimize the wastage.

Institutes can charge students and staff for the printing done over and above the quota allocated.

This will encourage the responsible use of printer and give freedom to use the printer for use for which students/staff are accountable and Institutes can generate some additional funds for re-allocation to technology upgrades.

Scheduling Quota
By scheduling the Internet access, Institutes can limit access to students during the business hours, and give faculty members high priority access. It also limits the time online.

Filtering and blocking access
It helps to

1. Limit access to
*   E-mail, chat, newsgroups, or combination of them
*   Music and Entertainment sites (Streaming media files) - enables students to enjoy music and other large file transfer while critical traffic performance and security is not sacrificed
*   Sports

2. Prevent access to
*   Images of graphic violence
*   Sites (URL) and keywords that Advocate violence, criminal/illegal activity such as gangs, illegal drug use

3. Contain potentially inappropriate or bad language
*   Classified as "inappropriate" for students and similar material.

Challenge 1
Limit time Online/hours of Internet time/Set surfing quota

Different students have different surfing requirements. Some students might require Internet access throughout the academic year while some might require only for a few months. Again, the computer center will be open only for approx. 12 hours a day, which means 12 hours are to be distributed among all the students in such a way that it does not generate any dissatisfaction and all get their fair share.

*   Identify students
*   Determine the total time required
*   Determine the surfing needs
*   Set User surfing quota according to the needs dentified
*   Daily Quota restricts surfing hours per day
*   Weekly Quota restricts surfing hours per week
*   Monthly Quota restricts surfing hours per month
*   Yearly Quota restricts surfing hours per year
*   Define Surfing Quota policy for the identified students E.g. Can access for 2 hours daily throughout a month

How it works:
Allows Users to access Internet access only for the allocated time and blocks access after time quotas are exhausted.

Challenge 2
Restrict/Schedule Internet Access

*   Identify student
*   Identify access time needs
*   Set schedule based on day of the week and/or time of day
*   Define Internet Access policy for the identified students that restrict access: Allow/Disallow Internet
*   access within certain defined period i.e. allocates a certain amount of time when students can access Internet E.g. can access from 12 AM to 2 PM only.

How it works:
Restricts Internet access based on the time or day of the week.

Challenge 3
Block access to inappropriate sites, word, and/or images

*   Deny/Allow the access based on web categories like graphic violence - violent images, language, bomb-building, etc.
*   Sexually Explicit
*   Criminal activities - promoting illegal activity
*   Other Categories - alcohol, games, advertising, politics, sports etc
*   Identify sites
*   Identify Content types
*   Identify file types
*   Define Web category with site names, file types, keywords
*   Define Security policy and attach Web category

Can also be used to block

Heavy downloading of Audio/Video files like MP3, Winamp, Real Audio, Media Player and

Virus signatures to protect Network against the malicious virus attack.

> Web category is the grouping of URL keywords for Internet site filtering.
>
> Cyberoam allows to categorize Web sites such as Games, Music, Chat etc.. Once the web sites and contents are categorized, access to those sites and contents can be controlled through policies.
>
> Depending on the requirement, allow or deny access to the categories with the help of policies by groups, individual user, and time of day.

Challenge 4

Schedule based filtering

Assign filtering based on a particular time of day. For instance, the most restrictive filter can be applied during the working hours

while relaxed filter can be assigned during the lunch hour or after working hours.

Challenge 5

Assign printing quota to reduce the wastage

- Identify students
- Determine the printing needs
- Set student quotas using Printing policy
  - Daily Quota
  - Weekly Quota
  - Monthly Quota
  - Yearly Quota

- Can also set Special User printing policy with no restrictions at all

Monitoring the Usage

How would you check whether the policy implemented is right and in tune with your requirements?

Cyberoam provides the easy-to-understand & interpret graphs to check the impact of policies and monitor usage:

- Check Web surfing graphs
- Check Internet Usage reports
- Check Student/staff wise and Content wise Data transfer graphs
- Check Student/staff wise and Content wise Internet usage graphs
- Check the trends

Cyberoam records the information about the usage based on the actual surfing done. This information can be used to:

- Determine the heavy usage periods
- Spot Abusers
- Increase or decrease the surfing limit
- Reschedule the access
- Charge against students/staff for usage if required

Conclusions

In summary, there is no easy, single step solution to managing the Internet access.

The threats to an Academic Institutes are highly varied both in their nature and in the medium of exposure. Furthermore, the nature of these threats is constantly changing; a change driven by external forces and by the evolving nature of how students use information.

However, just like virus scanning, managing the Internet access is an ongoing process. Although a strategy needs to be developed, it is essential that flexibility and adaptability remain the cornerstones.

How Cyberoam Can Help

Cyberoam presents an integrated approach to managing your Institute's IT resources. Robust Internet scheduling, filtering & blocking, allows you to protect your Institutes and maximize use of your assets.

Cyberoam filters and monitors your Institute's entire Internet access using simple policies combined with the list of pre-categorized Web sites.