Overview  *(Feel free to add/edit/omit any section)*

This policy sets out critical guidelines covering the use of mobile devices for learning purposes in *(Formal in-class)* and *(Informal out-of-Class)* settings. Adoption of such policy should protect educational institutions against wrongful use of mobile devices. Institutions should consider adding an additional policy terms if a particular institution has unique and special requirements pertain to their particular settings and school culture. The policy is intended to protect students, teachers, all stakeholder also security and integrity of data and technology infrastructure. Most school systems have not found a sustainable way to provide the same device for all students. Schools often do not have an infrastructure for allowing an entire school population to access the Internet without adding costly Wi-Fi access nodes.

Policy challenges

Policy challenges includes but not limited to the followings: standards, acceptable devices, sets of procedures, safeguards, third party app usage guidelines, software security, data protection, enforcement of regulation and
proper/acceptable use (Khaddage et al, 2015). School systems have challenges as well in trying to embrace the mobile learning experiences. Funding is a potential for additional distractions from learning and concerns about student Internet safety (Project Tomorrow, 2011). More recently, district personnel concerns regarding equity have grown even larger (Project Tomorrow, 2014). There is a need to develop policy guidelines for equitable access, privacy, and frustrating, wasting instructional time. This issue is compounded in locations where high-speed access is cost-prohibitive or completely unavailable (ITU, 2010). Many school systems are considering “Bring Your Own Device” (BYOD) strategies that entail additional challenges for educators. When students bring their own devices, variability in the accessibility and applicability of learning is problematic for teachers’ planning of instruction. However, most institutions currently have a policy prohibiting students from using their own personal mobile devices. In a principals were asked about their major concerns with accommodating student owned mobile devices at school. Their issues included concerns about theft of the devices and responsibility of that loss, concerns about network security, concerns about equity for those who have personal mobile devices versus those who do not have the devices, concerns about lack of teacher training to integrate the variability of mobile devices, concerns about the intellectual property, e-waste, and health and safety at the local, national, and international levels (Lai, Khaddage, & Knezek, 2013) (Khaddage et al, 2015). These challenges are very much related to one another. Any new technologies lead to new pedagogies, new policy and new research; We need an innovative approach not only in the creation of new, authentic pedagogies, policies, and research but also in the action learning techniques that can be adopted when selecting the appropriate technologies and the relevant content to suit everyone. By doing so we could make an initial plan easy to incorporate and follow, and also important issues won’t be left out, hence increasing the chance of seamless implementation. Addressing informal learning is considered quite important (since we are dealing with ICT), so as to connect learning between formal and informal contexts, we also need to identify barriers that inhibit bridging formal and informal learning through ICT.

Recommendations

Educational institutions are still fretting about mobile learning (policies as well as pedagogies, research and technologies) and struggling to find ways of proper integration. The student-Centric finds that the gap between personal and study devices are yet to be made clear to all stakeholders. Bring your own device (BYOD) programs call for three critical components: a software application for managing the devices connecting to the network, a written policy outlining the responsibilities of all stakeholders (students, teachers, administrators, parents) and an agreement all stakeholders must sign, acknowledging that they have read and understand the policy. Sample questions that must be settled by educational institutions and should involve all stakeholders during the planning stage include: Which web browsers should students use? Which security tools offer the best protection for the range of devices (if BYOD) was the proposed method? What level of support is IT expected to provide? What PD (professional development) strategies will be followed and adapted? To make sure nothing is overlooked, get input from all stakeholders evolved. A draft policy outline that can be adapted to suit their needs can cover the followings:

Acceptable Use

- The educational institution should define acceptable use as activities that formally or informally support students’ learning.
- The educational institution should define what is considered acceptable personal use on time as reasonable and limited personal communication or recreation, such game playing for entertainment.
- Students as well as teachers should be blocked from accessing certain websites during school hours/while connected to the corporate network at the discretion of the institution.
- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)
- The following apps are not allowed: (include a detailed list)

Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
Connectivity issues are supported by IT

Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Security

Part of the problem with mobile devices integration in education is that they are vulnerable to more threats, from the device being lost or stolen, device being damaged, to inadvertent data leaks, and device hacking. In order to address and prevent these threats, two possible mechanizes within the policy should be considered:

<table>
<thead>
<tr>
<th>The human (all Stakeholder) factors</th>
<th>Enforceable policy, Educating all stakeholders is the most powerful tool for getting them to comply with mobile rules.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technological protection from the institution</td>
<td>Working with all stakeholders in order to limit exposure. Using a variety of tools to protect data &amp; data recovery on mobile devices. Encryption of data on devices, data loss prevention measures, listing apps and services, virtual &amp; cloud-based workspaces, devices must be password protected.</td>
</tr>
</tbody>
</table>

References


