

# Mobile Strategy for Binghamton University

---

## Binghamton University Mobile Strategy

### 1.1 Introduction

“Mobile phones will overtake PCs as the most common Web access devices worldwide by 2013.” –Gartner Group (one of the world's leading information technology research and advisory company.)

The world is shifting to a mobile-dominated post-PC era in information technology (IT). The research firm Gartner predicted mobile phones will overtake PCs as the most common web access devices worldwide by 2013.<sup>1</sup> This shift is enabled by the convergence of three trends: the growing number of Internet-capable mobile devices, continued development of networks that support connectivity and increasingly flexible web content.

Young adults, especially college students, are leading the shift to the mobile era. As more users from around the world gain Internet access via their smart devices, Binghamton University’s digital presence must adapt to better serve our students and other stakeholders around the globe. Using the latest technology, Binghamton University has built both a branded website framework and mobile app framework that allows users to access our content on a consistent basis across all devices.

It’s imperative that the University campus embraces the fact that we are setting the pace. It’s vital that we keep content flowing through a consistent location that is properly vetted, maintained and branded.

Binghamton University supports mobile web technologies that simplify user experiences, while at the same time keep pace with a rapidly evolving mobile landscape.

### 1.2 Audience for the Strategy

Campus Leadership, faculty, staff, students should be aware that mobile connections come in a variety of forms, and it’s imperative that all platforms and groups are taken into consideration when developing mobile-friendly content.

Connections made via a mobile platform can be as varied as alumni living in Binghamton to a prospective student in Bombay. There is a large market for mobile content and content strategy.

### 1.3 Goals of the Strategy

- Continually look to improve on the digital experience of being connected with Binghamton University.
- Increase the availability of mobile-friendly services. For example, pay a bill or register for classes.
- Reach for innovative ideas that keep us ahead of the curve of the mobile experience.

## 1.4 Strategy Stakeholders and Review

- Student Affairs
- Academic Affairs
- Information Technology Services
- Communications and Marketing
- Student Accounts

## 1.5 Current Situation

Below is an audit and assessment of the current status of mobile facilities, campus Wi-Fi, mobile websites (adaptive site), and mobile apps.

### Mobile Applications

- bMobi (iOS , Android)
- B-Reader (iOS Android, has not been updated since spring)
- Binghamton U Graduate School (iOS ,Android)
- P.R.I.D.E. Binghamton Rewards (Athletics) (iOS Android, Windows version?)

### Academic Systems (responsive/adaptive)

KEY: C - Complete; IP - In-progress; P - Partially (ex.: departments of a school live);

N - No Progress

- MyBinghamton Portal - N
- Banner - IP

### Academic Websites

- Homepage - C
- About/Visit - C
- Admissions - IP
- Alumni - C
- College of Community and Public Affairs - C
- School of Management - C
- Decker School of Nursing – C
- Graduate School - IP
- Graduate School of Education - C
- Harpur College of Arts and Sciences - IP
- Watson - C
- Continuing/Professional Education - IP
- Office of the Provost - C
- Office of Diversity, Equity and Inclusion - C
- University Libraries - C
- Advancement IP Student Affairs - P (3 of 20)
- Administration - P
- Research - N
- Athletics (bubearcats.com) - N
- Binghamton Magazine - N
- Inside Binghamton University - C

There are several other sites being prioritized for migration into responsive templates or are in-progress. The above list represents the first phase of migration priorities for calendar year 2013/14.

## **Campus Wi-Fi**

The campus wireless network consists of over 2,200 wireless access points. It supports 12,000+ concurrent users. There are over 30,000 unique devices registered on the wireless network. It supports 802.11 a/g/n protocols.

Wireless is available in every building on campus. Binghamton's goal was to make it pervasive throughout. Last summer we completed a full upgrade of wireless in the residence halls to the latest technology. Also this summer, we upgraded the lecture halls for dense wireless. Now we can accommodate a full lecture hall 1 (400+ people) all running wireless devices concurrently. This assists faculty in administering online tests and also for conferences.

The control point of the wireless was also upgraded to newer hardware and offers full failover redundancy.

### **1.5 Target User Groups**

Mobile technologies are transforming the way student's access academic information, impacting the University's educational mission. Going mobile has great potential to improve student communication, engagement and learning.

Mobile engagement can improve outreach to underrepresented communities. Cell phones help bridge the digital divide by providing Internet access to less privileged teens. 41% of teens from households earning less than \$30,000 annually say they go online with their cell phone.<sup>3</sup>

Currently all users of the Bmobi have access to maps, places on campus, directory, courses, library, events, news, videos, images, social media links, athletics news/scores/schedules, link to the responsive main University website, res life connection, grad school link, Blackboard, and emergency contact info.

User groups include current and future students, alumni, academic staff, suppliers, contractors, and parents students.

### **1.6 Infrastructure Requirements**

We are just beginning phase 1 of a 3-year process to upgrade the core areas of campus to newer technology. This will include increased density, faster speeds, and more redundancy. Some of the new hardware will support even faster 802.11a/c speeds.

Binghamton University has seen an unprecedented increase in demand for both Wi-Fi and Internet access across the campus. Although Wi-Fi signal has been made available in the interior of all campus buildings, the density of mobile Wi-Fi devices now needs to be addressed. Students, Faculty and Staff are carrying an ever-increasing array of wireless devices. It is not abnormal for a student to have a Wi-Fi capable, phone, tablet and laptop at their disposal. Faculty are beginning to conduct electronic quizzes and tests in the classrooms and students are now gathering and collaborating electronically in spaces that they could not do so before. To address this ITS is in the process of deploying an upgraded wireless infrastructure to support this increased demand.

We have also seen a continuous increase in Internet, with demand increasing at a rate of nearly 40% per year. To address this ITS has upgraded Internet capacity to keep pace with this trend.

To address the overall increase in Wi-Fi and Internet usage the backbone of the Campus network was upgraded in the summer of 2013, and the network infrastructure continues to be upgraded in a comprehensive manner.

## 1.7 Security

Binghamton University boasts a secure, robust Wi-Fi network in every building on campus. The residential living quarters are all Wi-Fi capable as well as all academic and administrative buildings.

The campus Wi-Fi network infrastructure is encrypted and has the ability to logically place students and faculty/staff on separate networks. This enables a security layer for administrative resources such as servers and shared drives that faculty and staff can access and that students cannot.

Binghamton University also provides an open wireless guest network named "Connect2BU." This wireless network was designed for use by prospective students and their families to connect to both the Internet and to campus informational resources, thereby enhancing their visit to the campus. It also serves as an on-boarding network for students, faculty and staff to provide easy to use instructions for connecting to the secure encrypted campus network.

### Risks

Any data that we currently categorize as sensitive should be considered at risk with mobile usage. There is no reason to create new categories of data based on how someone accesses them. Mobile devices (to include laptops) are simply small computers. The security risks with mobile devices are compounded partially due to the ease of loss/theft of the device and the open approach of some mobile operating systems. Technically, a USB memory stick could be called a mobile device for the purposes of data security discussions as someone can carry it in their pocket, use it to store sensitive data and carry it off campus just like with a phone, tablet or laptop.

Mobile devices are the number one targets of thieves today. This can come from devices that are physically stolen or their control stolen by infected or misleading apps.

A device that is physically stolen can have sensitive documents on it, access to critical apps such as e-mail, company applications, social media accounts, etc. Faculty members may have important research their device. Staff members may have downloaded sensitive documents as e-mail attachments or other services. Students may have financial documents or access to various social media on their device. Any of these on a lost device could fall into the wrong hands.

Like desktop computers, mobile devices can be attacked by malware or just misleading apps. Misleading apps can look safe enough but may actually be stealing data, or may leave you holding the bill for surprising charges. Malware disguised as a popular mobile application can perform nefarious feats, from taking control of a mobile device and running code from remote servers to tracking an owner's location,

all of which can give rise to significant privacy and security concerns. Many times these can be disguised as anti-virus apps.

Another area of concern is “Data leakage.” Many mobile users sync data to their various mobile devices through free services like Drop Box. These services can get exploited and allow the files to be corrupted or stolen.

There is an inherent difficulty in securing mobile devices in the new “Bring Your Own Device” (BYOD) environment. Standards can and should be set for University-issued devices but securing a personal device remains with the diligence of the owner.

A comprehensive website on safe mobile computing needs to be created. Some of the suggested standards for personal devices and should be mandatory for University supplied phones:

1. Locking – this is a capability supplied on all smart phones that makes someone enter a password or swipe the correct pattern on the touch screen. New phones offer biometric access measures.
2. Remote wipe capability – offered through iOS for iPhones. For other phones there are services that provide this capability. This allows someone with a lost phone to wipe out everything, i.e. files, apps, photos, etc. from a remote location. With a good backup in place the wiped items can be restored on the phone if found or on a replacement phone.
3. Malware protection app – the same carriers of malware that plague desktops also are a threat to mobile devices—infected websites, file-sharing services, e-mail attachments. Old versions of Android also leave security holes.
4. Shop reputedly – there are plenty of app stores claiming to have ‘the world’s widest selection,’ but independent app shops tend to be less regulated than those run by well-recognized tech titans like Google and Apple. Only authorize the downloading of apps from reputable vendors to circumvent the distribution of mobile malware into your organization.

A possible next level of protection would be encryption. This is a more dramatic measure where data on the phone is encrypted and cannot be accessed without typing in a password on power up. A risk assessment of possible loss should be undertaken to evaluate the need for this kind of protection.

Mobile devices such as smart phones and tablets can be set up to access most of the critical University communication services. Below is a list of the most popular:

- Any Wi-Fi enabled device will be able to connect to the BU wireless network. The website <https://wireless.binghamton.edu> has instructions to enable your device to access the network.
- Your mobile device can have its e-mail app setup to access the Universities B-Mail and calendaring.
- File sharing can be done through Google Drive on your b-mail account.
- In the near future there will be web-based access to a person’s personal H: drive.

It should be noted that if faculty/staff wish to share data with non-affiliated individuals they will not be able to use something like our enterprise file sharing system.

## 1.8 Other Risks

- Mobile devices being used to maintain/store personal data from research projects
- Mobile devices being used to maintain/store grades or other sensitive student data
- Mobile devices being used to photograph and share images of protected data, research projects, and intellectual property (ours or someone else's)
- Mobile devices being used to assist students with test taking (cheating)
- Stolen mobile devices used to impersonate University officials, faculty, staff
- Stolen mobile devices being used to access secure university resources (not just data, could be notes saved on the device with passwords, codes to access rooms, file cabinets, HVAC systems, camera systems, or you name it)

## 1.9 Governance

It's imperative that Binghamton University have a consistent and current grasp on the possible mobile devices that are in any app store that bear the University name. The mobile task force shall have the authority to rule in favour of a mobile app being put into use or put forth.

## 1.10 Support

University ITS help desk services will provide end-user support for mobile computing for the Campus community.

## 1.11 Standards

The user experience and branding of Binghamton mobile properties is of utmost concern to the University. One's experience of the University increasingly will be through one's mobile device. That experience must be excellent. User experience and branding should support:

- Consistency across all mobile websites and apps
- Excellence in form and function consistent with our premier public goals
- Follow existing standards developed through our content management system (responsive templates), current mobile app development platform, and other software development kits (SDKs)
- Unification of our mobile/web properties rather than creating disconnected "pieces" of mobile communication and services
- Proposals for new University mobile properties or projects should be brought to the President's Mobile Taskforce for review and approval (see *1.9 Governance*)

University web and software developers have moved to a "mobile first" approach to web development where web-based systems are being designed to be "responsive" in nature, i.e. display well on a mobile device. The goal that "Any system accessible via a desktop computer should have a component of access available to mobile devices" may not be completely attainable but should be strived for. Users will expect this.

## 1.12 Backend Systems

Backend systems that are in use by the University include:

- The University runs Ellucian's student ERP product, *Banner*. Banner is accessed by both students and staff to process various academic functions such as course registration, billing, admissions processing, financial aid to name a few. Banner provides a non-mobile web presence. Authentication is done through Active Directory and the web pages can be reached outside of the firewall. The University is looking at options to make the Banner's web presence responsive. A possible alternative for the pages that don't adapt well to the responsive code is to develop Banner web services to be consumed by our existing mobile app, bMobi. Security of SIS data is of paramount importance as this development advances.
- Binghamton uses Blackboard's learning management system for both faculty and staff. This also uses active directory and can be used outside of the University firewall. Blackboard provides a mobile application for its product that Binghamton has purchased and which is accessible from the University's app, bMobi.
- The University runs Ex Libris *Aleph* product to handle it's library processing. There is currently a mobile application being written to support this product.
- The University runs several different smaller systems that support specific functions on campus. At this point most of these systems don't have a mobile component. However, the systems that deliver heavily used services should be prioritized for mobile development.

## 1.13 Mobile Service Delivery

Our current Mobile Service delivery is in a hybrid mode. We have responsive website pages and a native app. Currently having a responsive website that adjusts to any device is the best way to ensure a usable and effective mobile presence.

### 1.13.1 Off-the-shelf apps

Companies like Ellucian and Blackboard offer off-the-shelf mobile apps that can be branded and customised. Yet, our goal is to not divide the University online presence any more than necessary, rather to unify our offerings to our varied constituencies.

### 1.13.2 Custom Apps approach

In this prioritized order, always offer

- responsive web first,
- next hybrid cross-platform apps,
- and then native only if absolutely necessary.

### 1.13.3 Tool, Supplier and Method Selection

The Communications and Marketing web team has led the development of our current responsive web templates that are gradually proliferating throughout our web presence. They have also been the lead developers of the bMobi app. This team possesses key skills needed to develop and implement mobile properties. Yet, the rapid growth of mobile device adoption requires even more expertise and effort in developing mobile properties. Implementation and quality assurance testing are two areas in which ITS expertise is particularly needed.

#### **1.13.4 Skills Development**

Communications and Marketing staff have successfully led creative design, user experience (UX), information architecture (IA), implementation, testing and training in critical mobile areas to-date. ITS partnership has been critical to these successes. Continued success should build on existing skill set strengths in an increasingly cooperative manner.

#### **1.13.5 Mobility Roadmap**

- Responsive web first for all University websites
- New technical functions should be built into responsive sites (ex.: interactive map, virtual tours, orientation checklists, applications for enrolment, etc.)
- SIS and administrative systems, including payment gateways, should be made responsive
- Other key services should be brought to the web in a responsive format
- Key services should be provided via bMobi

Clearly there are far more potential projects than time to deliver them. Our first priority is to transform Binghamton's web presence into a 100% responsive format. Because of limited resources, the highest trafficked, highest impact sites will have priority.

We have created web pages to further explain mobile communications issues at this address <http://binghamton.edu/mobi/strategy.html>. Additional information about priorities and development efforts can be found in those pages.