Student Safety on Campus: A Guide to Mobile Access in Higher Education
Why consider mobile access for your institution?

Today’s colleges and universities demand secure and flexible solutions, not only for safeguarding people, assets and data, but for connecting students to services and applications campus-wide – from physical facility and logical network access – to cashless payment and tracking time and attendance.

In light of these developments, using a smart device for controlling physical access (what the industry calls ‘mobile access’) is a logical step for education institutions.

This eBook will focus on the benefits of mobile access in the new mobile-first world, help readers to understand exactly how it works and discuss what colleges and universities need to consider when implementing a mobile access control solution.

1 Experian Marketing Services, Millennials Come of Age, 2014

Smartphone usage (by generation) during a typical week around the world:

- Millennials: 765,919,000
- Generation X: 557,578,000
- Boomers: 499,866,000
- Silent generation: 60,845,000
Globally, smartphones are the most commonly-owned device (91%) around the world. Additionally, mobile devices are now internet users’ primary tool. Not only do 16-24s say that smartphones are their favorite gadget, since 2014 they have overtaken PCs and laptops as the most commonly owned device among this age group. It is also estimated that by 2020, almost three-quarters of the world’s population – or 5.7 billion people – will subscribe to mobile services.

A new class of devices called ‘smart wearables’ will increase the number of mobile devices in the market even further. These additions to the smart device universe include glasses, watches and fitness and healthcare devices. IDC predicts there will be 155.7 smart wearable devices in use by 2019. These truly mobile, ‘always-on’ devices are even more natural candidates for access control applications because of the ready-to-use convenience of a wearable device.

1 Gartner, news ‘Gartner Says Demand for Enterprise Mobile Apps Will Outstrip Available Development Capacity Five to One’, June 16, 2015 (Report: “The Enterprise App Explosion: Scaling One to 100 Mobile Apps”)
2 CompTIA, Building digital organizations, June 2015
3 GSMA, Mobile Economy Report, February 2017
How does mobile access work?

1. Administrator manages users and mobile IDs via the **Secure Identity Services portal**

2. Mobile ID is transferred to a user’s phone over the air

3. Reader is activated through a close proximity ‘Tap’ or longer distance ‘Twist and Go’ experience

4. Reader sends credential data to panel

5. Student is granted access to the facility by the control system
Driven by convenience and operational efficiency, educational institutions are increasingly seeking to leverage the potential of a mobile-first world. Universities must manage their students’ expectations for constant, instant access to buildings via their mobile devices. After all, 98% of millennials aged 18 to 24 own a smartphone, and 47% say they “couldn’t live without it”.

Harnessing the mobile revolution for physical access control will eventually merge the network and other secure access needs, creating a more connected environment.

Extending physical access to mobile devices increases operational efficiency by automating and eliminating some manual tasks. Consider how it changes a scenario that plays out in buildings all over the world each day.

1 Nielsen, Millennials are top smartphone users, 2016
2 Hill, C. Millennials engage with their smartphones more than they do actual humans, 2016
The benefits of mobile access

A better, more convenient student experience

The freedom to move access control to phones, tablets, wristbands, watches and other wearables offers choice and convenience to students, along with new and more convenient ways to open doors and gates.

• Because mobile devices are always on hand, students do not have to maintain and carry multiple cards.

• Access with a mobile device can offer a quicker and smoother experience. In schools’ visitor parking or at security gates, for example, the longer reach of the Bluetooth Smart communications standard makes it possible to drive up to the gate without having to roll down the car window and reach out to activate a reader.

• Smart device sensors, most notably the gyroscope and accelerometer, enable gesture detection. This offers an additional benefit for access control: the ability to open doors from a distance by performing intuitive gestures. For example, HID Global’s patented ‘Twist and Go’ technology allows students to unlock doors or open gates by rotating their smartphone in a way similar to turning a key. This also provides an additional layer of authentication for added security.
Mobile access can be more efficient to manage

Smartphones and mobile devices introduce new ways to manage mobile identities in near real time.

- **Time savings:** Using a cloud-based portal to centrally manage mobile identities instead of managing physical badges frees up time for administrators. It is even possible to enroll many users at once by importing a CSV or Excel file (batch upload). Invitations and provisioning to students can also be managed via email.

- **Simple enrollment for students:** A student receives the request via email, downloads the app and enrolls. The Mobile ID is provisioned straight to the student’s smart device.

- **Management of multiple locations:** Some universities have many campuses with different access control systems. With a mobile access solution supporting multiple identities per mobile device, a visitor can simply receive a new mobile identity on their phone before leaving or upon arrival.
Mobile access can be more secure

Mobile access complements existing access control solutions by enabling the use of a smart device as an alternative to more traditional form factors. Smartphones or other smart devices provide a number of security benefits over smart cards or fobs:

- Because smart devices can communicate with readers over longer distances, the readers can be mounted on the safe side of a door, minimizing the risk of theft, physical attacks or observation.
- Cards and badges are much easier to lose than smartphones. Mobile phones are rarely shared in a campus environment - something which happens more easily with cards.
- In the event of a lost, stolen or compromised mobile device, mobile IDs can easily be revoked for all access rights remotely through the management portal.
- Smart devices also support multi-factor authentication, biometric identification and other advanced security features that extend far beyond the capabilities of legacy cards.
The dangers of using outdated technology

Despite the availability of newer options, most colleges and universities are still using outdated and vulnerable access control technology. For these educational institutions, the time has come to prioritize plans for a much-needed upgrade.

Personal identification numbers (PINs) used by older keypad systems are easily shared and legacy systems, such as Magstripe and low-frequency proximity cards, are vulnerable to cloning (record and replay). Magnetic stripe (Magstripe) typically uses little or no security protections. Additionally, off-the-shelf devices are widely available to encode Magstripe cards. The adoption of PINs and Magstripe low-frequency cards has decreased due to the convenience, security and increased memory available in contactless smart cards.

In quality mobile access solutions, digital credentials like mobile IDs are securely stored and protected, utilizing the security features of the mobile operating system (e.g. sandbox or PIN) and strong encryption. Data is transmitted over the air through secure communication protocols and trusted back-end services, independent of communication technologies such as NFC or Bluetooth.
Mobile access enables a more connected environment

Today's educational institutions are beginning to see the benefit of merging physical and logical access. Simplified management, reduced expenses of maintaining multiple systems, improved security and enhanced user experience are driving this trend.

Smart devices can deliver additional security options for accessing data networks by enabling multi-factor authentication. They can generate other security features, such as the one-time passwords required for accessing the networks or web-based applications.

Students can conveniently use the same device for building access, VPN authentication and wireless network access, as well as for logging into the university intranet, email server and other IT resources.

A shared mobile identity platform for both physical and logical access has several benefits. It makes it easier for security administrators to manage access rights, reduces errors resulting from improper synchronization between two separate management systems and offers greater convenience for students to authenticate to different services.
Conclusion

Mobile devices are changing the way that students work and how educational institutions think about their operations, networks and security. The logical next step for many institutions is to replace legacy systems with future-proof and flexible physical access control solutions that support mobile access.

• Putting mobile devices to work as tools for access control is more convenient for students.

• Mobile access is more efficient for educational institutions to manage and more secure than previous generation technologies.

• Mobile access creates opportunities for the convergence of network and physical security that are unavailable with legacy systems.

To learn more about mobile access and HID Global, please visit: hidglobal.com/solutions/mobile-access.

If you have any questions or would like to request a call back from one of our Sales Advisors, please leave your details and we will be in touch.