

Software2

# The Ultimate Guide To BYOD And Off-campus Access



## What is BYOD?

BYOD, or 'Bring Your Own Device' is an IT principle enabling users to use their personally owned device(s) within their organization's infrastructure. BYOD is often achieved through leveraging technologies such as virtual desktop infrastructure and intranet systems to allow access to organizational software, file storage and networks. The phrase BYOD is frequently used (perhaps slightly erroneously) to mean on-demand and unrestricted access to software, particularly off-site access.

The ultimate guide to BYOD details the commercial and technical effects of enabling BYOD in universities and goes into depth on the technologies involved. This guide will cover:

- the benefits of Higher Ed BYOD, both commercial and technical
- How do I get started with BYOD?
- What technologies do I need for BYOD?
- How much does BYOD cost?
- What are the benefits of BYOD?
- what's possible with BYOD



# Table of Contents

An introduction to BYOD	3
What are the benefits, limitations and challenges of BYOD?	15
How to implement BOYD	19
How to get the most out of BYOD	26
Software Delivery Glossary	33



# 1. An introduction to BYOD

## What is BYOD?

When it comes to software delivery, BYOD, or 'Bring Your Own Device' is a principle enabling users to access their organization's software on their personally-owned devices. They may do this on-site or off-site and both of these contexts have different needs when it comes to the technologies used.

BYOD is often achieved through leveraging a powerful delivery technology, capable of covering all possible contexts of the end-point and of the user requesting software. The main underlying technologies frequently used to enable and provide BYOD include application virtualization, VDI, direct downloads, and hosted/online applications. Some universities even hand out devices to students to encourage BYOD; they might be Windows laptops or thinner clients such as Chromebooks. The phrase BYOD is frequently used (perhaps slightly erroneously) to mean on-demand and unrestricted access to software, particularly off-site access.



## Why enable BYOD?

BYOD carries with it a good number of significant benefits as well as challenges, which we'll go into in greater detail throughout the rest of this guide. However, even without dissecting why you should or shouldn't choose BYOD at this point in time, it is unquestionable that allowing students to access university software on their own personal devices is the future of more agile software delivery.

So what do we mean by 'agile software delivery' and why do we need software delivery to be agile? To truly enable BYOD, we must be able to deliver software to users regardless of their situation. Software delivery technologies tend to be very capable for specific use cases. For example, imaging allows for the uniform installing of software on hundreds or thousands of devices. VDI allows cross-platform delivery or delivery to zero or ultrathin clients. In order to deliver to multiple contexts, it is often necessary to use different methods for different situations, and that is what is meant by 'agile software delivery'.

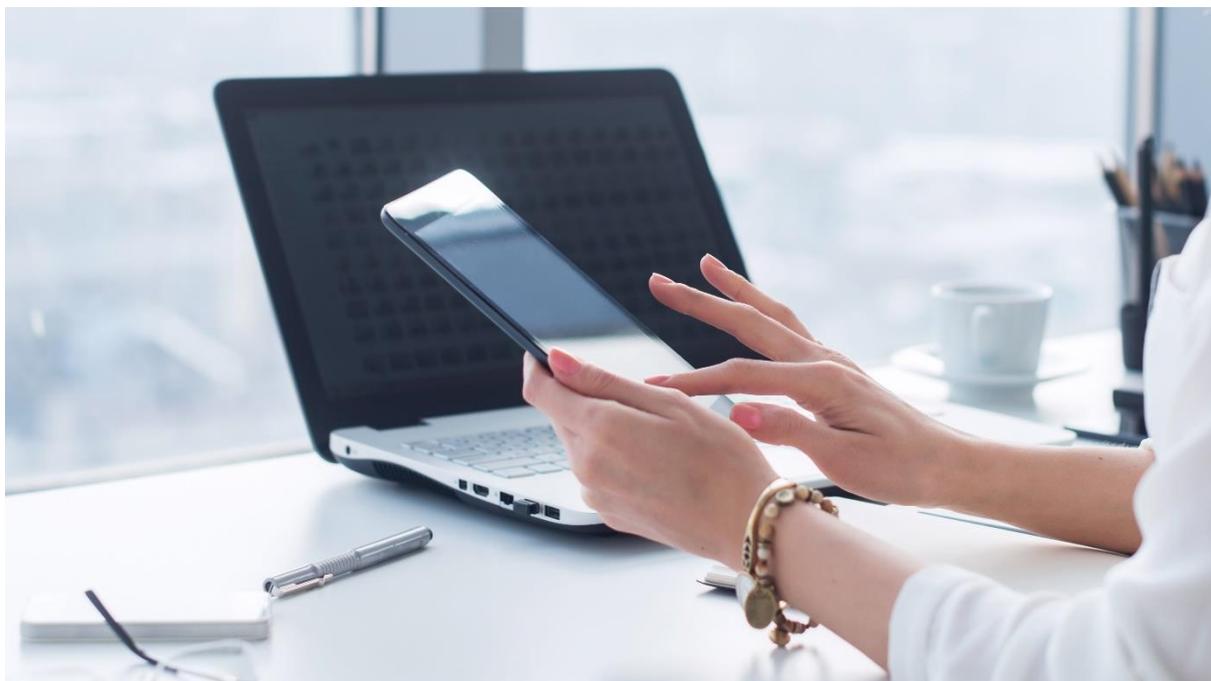
Not only does BYOD solve problems and fulfil use cases for more effectively delivering software to students during their university experience, but it also helps to prepare them for what is swiftly becoming the new standard for the world of work.

In Higher Ed, BYOD is often regarded as one of the top strategic IT drivers that matters to CIOs. IT decision-makers across the planet see BYOD as a vehicle for delivering positive change to students and staff, both on and off-campus. Increased flexibility and mobility that's brought about with a coherent BYOD strategy can drastically improve how students consume university IT services, and with it, an improved student experience.



## **2. What are the benefits, limitations and challenges of BYOD**

## What are the benefits of BYOD?



### For Students And Faculty

- **Familiarity and productivity:** Your users, whether student or staff, are able to work on the device they know best, with the hardware they're used to and the preferences and settings of their choosing. With more familiarity with the keyboard, trackpad, mouse, or other control devices, comes a higher potential for productivity, enabling faster work and a better user experience. In the same vein, users will be working with their own personal preferences; preferences they have chosen to improve their workflow. For example, shortcuts such as taskbar thumbnails or hot corners on Macs enable efficient multitasking and switching between programs. Personalization options such as text size or dark mode make on-screen information easier to digest. The list goes on.

- **Convenience:** Being able to access university software on personal devices means less time spent traveling to labs or campus facilities just to complete course work or planning for lectures and seminars. Students and faculty no longer need to account for rush hour periods in order to secure a machine.
- **Flexibility:** Personal devices and, by extension, software applications will always be available to students and staff whenever they need it. Last-minute changes or minor tweaks to digital work become easily possible and users can work in a more agile manner. That allows them to achieve more in their education, as well as their extra-curricular activities.

These benefits for students and faculty all directly translate to commercial benefits for universities. A better student experience results in higher grades and a higher approval rating from students, which in turn will facilitate higher grades, higher university rankings, greater enrolment figures, and more revenue through student retention.

Equally, providing everything staff and faculty need to teach and research in their preferred way, supported by software access rather than contending with it will increase employee satisfaction and retention rates, resulting in happier, more productive educators.

## For Students And Faculty

- **Less hardware to manage:** Leveraging student and staff-owned devices means that device-management workload and investment requirements for university-owned hardware can be greatly reduced. Not only can this directly translate to commercial and financial benefits for IT departments, but it can allow more time to be spent on other strategic projects.
- **Fewer support tickets:** On two fronts, support tickets have been seen to reduce in number when BYOD is enabled: Students and faculty are working on their own machines, they are

more familiar with how to use them and how to setup software for them, resulting in fewer requests for support on those machines. Secondly, their experience in accessing software will remain consistent on their own machine, whereas it may differ on various machines from lab to lab. This means users can quickly learn the process and become familiar with it.

- **Less time spent imaging:** If a university is using VDI to enable BYOD, imaging is still required for some virtual desktops, however the need to image machines is greatly reduced if IT is using fewer machines! Imaging is laborious and time-consuming; reducing the amount required frees up more time to spend on other projects and introduces previously unheard-of agility and versatility in making changes to software availability mid-semester, such as updates, patches, and additions.
- **Less money spent on operating system licenses:** BYO devices' operating systems are pre-licensed by the owner of the device, and with users keen to keep their devices up to date, OS upgrades will be handled by them! Saved money can be redirected to other projects and areas of IT to continue providing the best digital experience possible.

Commercially, BYOD has the potential to make an enormous difference to universities in reducing their overheads and allowing them to use funds to improve services. For example, even in the case of only 20% of users being able to provide and use their own device, that represents a 20% reduction in the investment required to provide software to students through managed hardware. Using application virtualization to deliver software could also introduce a 20% reduction in expensive VDI seats/licenses and, if using products such as [Parallels RAS](#), a 20% reduction in server requirements.

## What are the drawbacks of BYOD?

### For Students And Faculty

- **Users without devices:** Users without their own devices may actually find a fully implemented BYOD policy more inconvenient. If their university implemented BYOD with the view of decreasing their investment in end-point hardware, a reduction in lab machines may make accessing software more complex and difficult to organize around university schedules and schedules of other students. [However, 95% of university students own a laptop](#)
- **Low-spec devices:** Users with low-spec devices may suffer when using certain delivery technologies. An example of this is application virtualization which leverages the hardware of the end device. Depending on how apps are provisioned and the technologies in place, some users may find it tough to access more demanding software.
- **Storage:** Users may have to use up their own storage to install and run apps. If they're running low on space already, this could affect the performance of software titles, whether they can run at all and, ultimately, the user-experience they receive.
- **Network connection:** Some BYOD technologies require a constant and strong network connection, with software title performance relying directly on connection speeds. VDI is a prime example of this where the compromise for its capability of running software on zero clients or ultrathin clients is the fact that a network connection must be maintained.

## For Students And Faculty

- **Security risks:** Allowing access to university systems, and services through and network connection on unchecked and unmanaged machines carries risks. If the endpoints are infected with malware, there is a chance for this to further infect university systems. Furthermore, users with malicious intentions or [RDP brute force attacks from external sources viruses present a higher risk](#) than non-BYOD software delivery policies if not managed properly.
- **Tricky licensing:** One of the toughest aspects of providing a great user-experience and consistent access to software through a BYOD policy is adhering to the license agreements of thousands of software titles. Some vendors are notorious for their tricky license stipulations, such as not permitting their software to be run off-site. There are multiple solutions for almost all of these clauses, however, dealing with them all may introduce another layer of complexity. Adobe, for example, doesn't allow their software to be used on VDI sessions. Software2 is experienced in dealing with difficult license clauses and AppsAnywhere has been designed around the complexity of software license agreements.
- **Provisioning for different devices:** A multitude of devices, operating systems, and hardware capabilities will need to be accounted for in a BYOD policy. This can greatly increase the complexity of logically provisioning software applications and deciding which delivery technology is best to leverage in any given situation.
- **May need to provide devices to some users:** As covered above, a portion of users may not own their own devices, or have a device that is insufficient for handling certain software titles. If lab/campus machines are reduced as part of a wider BYOD project, then IT may need to provide more managed devices (usually laptops) to students. This could be in the form of a student laptop loan scheme, for example.

- **Initial increase in support demand:** The introduction of new tools/methods of accessing software can often result in users feeling unfamiliar with how to use them. This may be compounded by the fact that a BYOD policy has to account for so many different devices and operating systems. Because of this, there may be more 'teething issues' than with implementing new delivery tools to managed devices, however, the nature of BYOD and students using their own devices mean the support demand will level out and often greatly reduce. Providing a consistent, clear, and centralized platform through which all your end-users can access their software will help with this.
- **No access to end devices:** With the previous point in mind, providing support and troubleshooting issues may be trickier without physical access to the machines for support/troubleshooting. Obviously, technologies such as remote access tools can be used, however, this is still a less straightforward way of providing support and may even be rejected by a certain number of users.

## What are the challenges of BYOD?

### Implementation

- **Multiple technologies can be required:** One of the most daunting parts of implementing a BYOD policy is that numerous technologies need to be used in combination in order to facilitate the wide variety of end-devices and user contexts that will be encountered. Without proper management of delivery technology licenses and smart contextual provisioning, this can get expensive quickly. It can also become very complex without the use of back-end provisioning tools.

Without front-end tools for users to access their various apps, the user-experience can become more complex and suffer, impacting student and faculty productivity and

increasing support demands. On closer inspection, however, the technologies required are likely already a part of most universities' software delivery stacks and perhaps are just more compartmentalized in their use, for example perhaps only using VDI to deliver cross-platform, rather than also using it to overcome licensing complexities. Amending the use of these tools can not only enable BYOD, but help to greatly reduce the investment required in each tool individually and manage/providing information on concurrent usage of software titles.

- **Data collection on available devices:** To get started, you'll need information about the devices you'll be delivering to and the number of each device. You may already have some data on this, but if not a survey or audit of student and faculty owned devices would be beneficial. It is also worth noting that there may be a degree of trial-and-error to this process and there is nothing to stop you tweaking provisioning and delivery methods based on what actual usage of a BYOD delivery estate looks like in practice.
  
- **Upfront investment:** Long term, a BYOD policy can reduce the investment required in hardware to provide software to your students and can right-size your use of existing delivery technologies. Over a period of months and years, money is saved but an initial investment will be required. This will mainly come in the form of signing license contracts with delivery technology vendors and investing in the necessary server infrastructure for delivering to student and faculty owned devices. This investment will vary depending upon the delivery solutions and infrastructure you already have in place. Many universities have found that trying to use VDI as a one-size-fits-all solution to BYOD is extremely expensive and not at all scalable. This is one of the reasons that many universities were initially put off BYOD and they may not be aware that the technologies to make the benefits far outweigh the costs exist today!

## Maintenance and Support

- **Supporting a wider range of different devices:** Supporting more device types means more user contexts and potentially more compatibility issues. This will need to be considered when implementing delivery technologies for BYOD and when provisioning applications using those technologies.
- **Support may require fixing pre-existing issues:** With users accessing university software on their personal devices, IT may experience support requests that are down to pre-existing issues or settings/preferences on the endpoint. This could result in IT having to spend a fraction of support time fixing issues on personal devices which are not IT's jurisdiction.
- **Have to maintain more services/technologies:** More technologies in use means a wider skill set is required for maintenance, support, and upgrades. Whether this comes in the form of upskilling staff or adding specialist members to the team, you may need to invest a little more in staff resources.

## Security

- **VPNs required to keep data secure:** A few more extraneous third-party tools may be required to maintain security, such as VPNs. The degree this needs to be used depends entirely on your specific delivery technology estate, but it is worth factoring in the investment and workload of using VPNs when approaching and operating a BYOD policy.
- **More frequent checks for malware required:** In a similar vein to the previous point, it may be necessary and is good practice to more regularly run system tests and checks for any malware or breaches of security. Generally, more diligence is advisable when it comes to any kind of attack, such as brute force attacks when using solutions like RDP for example.

## Licensing & Concurrent Usage

- **Some vendors license agreements are limiting:** There are many software vendors notorious for their tricky and limiting license agreements. For example, this may come in the form of 'named user', which prevents IT from assigning users a license from a 'pool' on-demand, or a license agreement stipulation which prevents software from being run and executed on off-campus hardware. This must all be considered in enabling BYOD and may call for some stricter provisioning conventions or access rights. It is, however, worth noting that some vendors are beginning to take notice of this challenge for higher education IT; they are aware that a strict and limiting license agreement may incite universities to go elsewhere for their course software, or reduce their spend with that particular vendor and offer their software to fewer student groups. This may come in the form of choosing device licenses over site licenses.

**Users may stay logged in and use up licenses:** There are many ways in which users may use up licenses even while not using software. They may leave their machine running, not close programs, or not maintain a network connection. This may be done innocently or in a direct attempt to keep software running. Often, delivery technologies have encountered this and have built-in ways of dealing with it, such as requiring a server connection periodically. However, it is still worth bearing this in mind and balancing license availability with user-experience, as, if these measures are too severe, it may result in a user being ejected from their software and losing work before saving, which is a staple of bad user-experience. While certain delivery technologies are historically more guilty of this than others, using the right control tools, such as AppsAnywhere, can help make lost work a thing of the past.

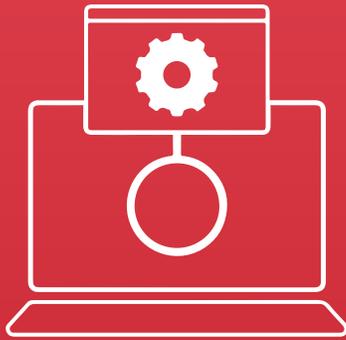
- **Different licenses to deal with:** The more technologies in use, the more licenses to invest in, track and update. Individual software title licenses are obviously necessary, as are operating system licenses. On top of this, application virtualization will need to be licensed to properly provide BYOD, alongside VDI licenses. VDI and RDP will make more CALs necessary, etc. You must ensure you factor in these ['hidden' costs](#) when creating a business proposal, or designing infrastructure for BYOD.

## See the AppsAnywhere user-experience

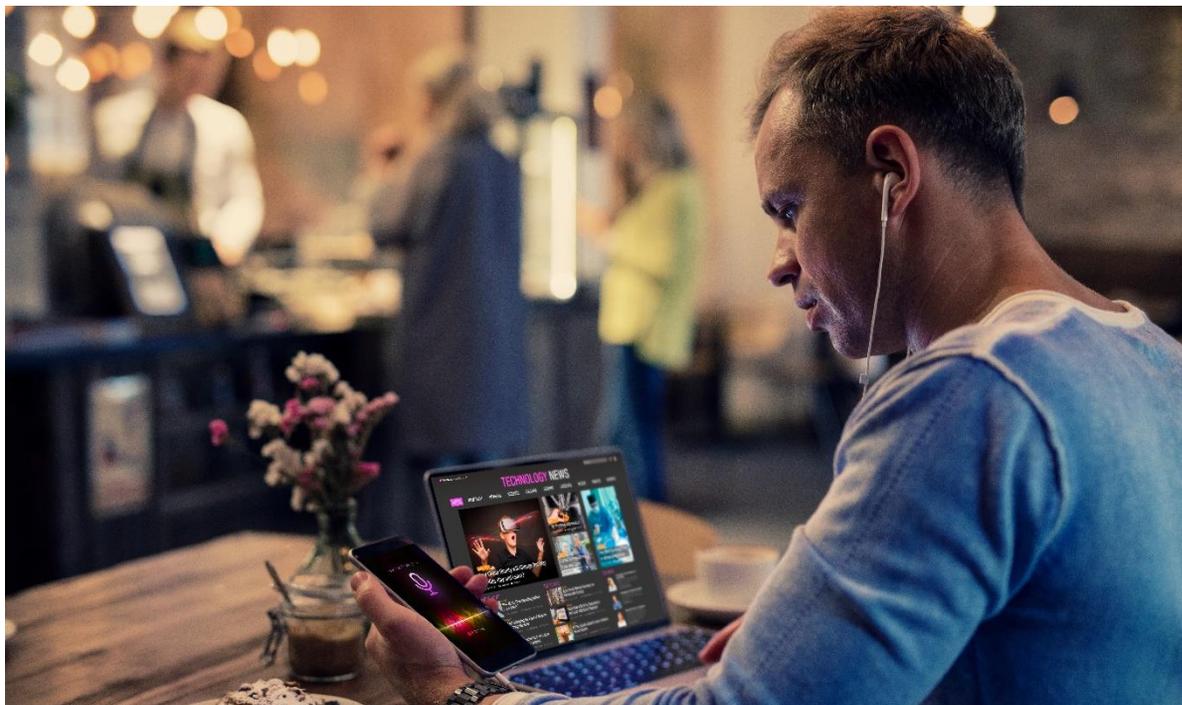
Trial the AppsAnywhere portal to learn how the world's leading higher education BYOD solutions is experienced by your end-users.

[TRY APPSANYWHERE](#)





## 2. How to implement BYOD



In order to implement a BYOD policy and provide off-campus access to university software, it is important to understand the benefits and limitations of the various technologies involved. When you're familiar with each technology you will be able to plan when and how to use each technology based on the context of delivery and prevent costs from quickly skyrocketing, all the while providing a brilliant student/user experience.

## Application Virtualization

Application Virtualization' is a software delivery technology that delivers applications inside a 'virtual structure' without the need for traditional installation on a per-device basis. Virtualized applications effectively 'stream' to the end-user device on-demand, leveraging the end-device's hardware. It differs from 'desktop virtualization' (VDI) in that only the application is virtualized, rather than the full operating system.

Application virtualization is a comparatively new addition to software delivery technologies and represents a natural progression from server and desktop virtualization. It has been widely considered to be 'game-changing' for IT departments both higher education and enterprise alike, and rightfully so. Its ability to virtualize applications inside a virtual structure, separately from the underlying operating system puts it in a unique position to solve a number of challenges. The application market has grown considerably in recent years in both size and advancement of technology. There are many more viable options than just App-V, many of which more capable, with vast improvements on the limitations of App-V.

- **Leverage the hardware of end-devices:** Application virtualization is executed inside a virtual structure on the hardware of the end device. This reduces the investment necessary in infrastructure hardware when compared with other technologies. This is beneficial for delivering non-heavyweight, licensed/paid applications to most modern devices. Application virtualization can also be very effective in delivering FOSS apps, however, it is advisable to deliver these through a direct download link to save your licenses for when they're needed. Another benefit of this is that virtual desktops aren't required, meaning no expensive VDI licenses or CALs to deliver software through application virtualization.
- **Doesn't require a constant network connection:** Because virtualized applications are run and executed on the end-devices hardware, they only require a network connection during the download process. This makes for a liberating user-experience, allowing end-users to continue using their applications in the event of disconnection or outage, as well as on-the-move in connectionless locations. This also means the performance of their applications isn't limited by the speed of the network they're connected to. A 'buffering-style' load and install of virtualized applications mean that they can be run before they are fully downloaded, with the essential parts of an application being downloaded first and further application components being loaded in later or as-and-when they're needed.

Given the advanced nature and flexibility of application virtualization, it should be considered the go-to technology for delivering licensed software to BYO devices whenever providing a direct download link or web version won't work.

There are traditional [key application delivery technologies](#), one of which being the legacy [Microsoft solution AppV](#), however, we recommend [Numecent Cloudpaging](#) as it is the leading higher education app virtualization solution and the only solution [capable of delivering 100% of Windows apps](#). You can read more and learn all there is to know about application virtualization in Software2's 'The ultimate guide to application virtualization'.

## APPLICATION VIRTUALIZATION GUIDE

# What is BYOD?

Virtual Desktop Infrastructure is a server-based software delivery technology that separates the operating system and desktop environment from the physical end-hardware it is to be accessed on. Applications compatible with the virtualized operating system may be accessed and executed on the virtual machine with a user-experience consistent with that of a traditional machine and operating system.

VDI is a heavyweight and powerful solution to software delivery problems that seem otherwise unsolvable. It can help circumvent strict licensing stipulations that usually render it impossible to deliver certain titles to user-owned devices off-site, and it can overcome endpoint hardware being insufficient to run more CPU and GPU intensive programs.

- **Run on-site, deliver off-site:** Often, one of the most significant obstacles to enabling BYOD is the license agreements for individual software titles. Many of which are notorious for including a condition that their application may only be run on on-site hardware. This renders application virtualization inapplicable and does not even permit physical install onto student-owned machines. This can begin to make things tricky, especially in the delivery of heavyweight applications. VDI provides a solution in that software is run and executed on university-owned, on-campus servers and then pixel-streamed to end-points, helping IT deliver software to BYO devices while fully adhering to license agreements.

- **Deliver heavyweight apps:** VDI doesn't rely at all on end-hardware capabilities, meaning even the heaviest of applications can be run on older or under-powered devices. Want to run AutoCAD on an older laptop with limited CPU RAM and no dedicated GPU? You can with VDI. As long as the network connection of the end-device can accommodate the pixel data required – and you have a large enough IT budget for hardware/server costs – there are no limits to what can be delivered using VDI.
- **Deliver cross-platform:** Another function of software not being executed on end-devices, but run on servers and pixel-streamed, is that IT can deliver cross-platform; ANY application to ANY device. We've even seen ArcGIS running on the dashboard computer of a Range Rover Evoque via a similar, pixel-streamed solution! It's for this reason that VDI is often the go-to solution for Higher Ed, so both Windows and Mac devices can be supported.



- **Keep sensitive data on-site;** Another benefit of VDI is that all sensitive data remains on-site. For any situations or policies where data protection and security, in general, are a concern, VDI may be the way to go.

So VDI obviously has its benefits and lends itself to many different challenges of delivering to off-site, user-owned devices; it almost sounds too good to be true. That's because, in a way, it is. VDI is extremely expensive and demanding from a hardware and staff resources perspective. It needs a lot of server infrastructure to run and specialist knowledge to maintain and install. Virtual desktops still need to be imaged, so this arduous and laborious task is not avoided and there are many ['hidden' costs to VDI](#), such as CALs. With this in mind, you should reserve VDI use for where it is absolutely essential; it should be seen as a complimenting technology to deliver the final 5-10% of apps to user-contexts where, without VDI, these apps would be undeliverable. Reserve your VDI use for the following situations:

- Cross-platform delivery
- Delivery of applications to under-powered end-points (BYO devices)
- Delivery of software with tricky license agreements
- **Situations where no other delivery technology will suffice!**

You can read more about VDI in Software2's 'The ultimate guide to VDI'.

[VDI GUIDE](#)

## Front end/access point

It's important to consider not only how an application will be delivered technically, but also the steps students/users must go through to find and launch an application. To the student, their experience with apps isn't granular and they'll view the performance of an app through the same lens as the simplicity and convenience of locating and launching it. Many delivery technologies feature front-end portals through which to access applications, but when multiple delivery technologies are in use, then each application will have a different route or set of actions necessary to launch it. This can be compounded even further when there are multiple user groups for different app sets or departmental software.

This is sometimes known as “portal sprawl”; the idea that students might need to go to multiple places to find their software, depending on the software title itself, their faculty, whether they're on or off-campus, and more. Students don't want to have to figure out where to get their apps, they just want to run them and for them to just work!

AppsAnywhere is the only solution allowing users to launch all of their apps from the same place. It presents the user with a menu of apps that can be searched for within the portal or arranged into app lists (which are then shareable by URL or via VLE/LMS such as Canvas).

No matter the delivery method or platform used to access, every single software title available to a given student is accessed through AppsAnywhere. Locally installed apps, virtualized apps, and apps delivered through virtual desktops all feature exactly the same user experience to launch. And all of this is done in a way that IT can set access restrictions to adhere to individual software title's licensing requirements.

Learn more about AppsAnywhere by clicking the button below.

[APPSANYWHERE](#)

# Cost of Implementation

## Licensing costs

Some of the most obvious costs to implementing a BYOD policy are the licensing costs you'll pay to technology vendors, however, some license costs you don't expect may crop up. Some consider these to be the ['hidden' costs of solutions, something VDI is particularly guilty of](#). Following is a list of the licensing costs you can expect to encounter while enabling BYOD.

- **Software title licenses:** Obviously, you will still need to license every software title you'd like to deliver to BYO devices. Perhaps slightly less obviously, the act of enabling BYOD has the potential to affect how many licenses you may require for each title. Popular and frequently used titles may see an increase in peak concurrent use due to their ease of access with BYOD. Conversely, any software title could also see a drop in peak concurrent use due to making access easier out-of-hours and off-site, with those who prefer to study and work later or earlier than usual hours choosing to do so. BYOD solutions, such as AppsAnywhere, may also offer some [analytics or intelligence on your software title use](#), allowing you to factor more real-time data into your decisions on how many concurrent licenses to purchase.
- **Application virtualization licenses:** Application virtualization is our recommended delivery technology; it's scalable, highly capable, and is the best solution for leveraging user-owned hardware. It provides the best user-experience of delivery technologies capable of facilitating BYOD and carries with it the highest potential commercial benefit for universities. The technology license costs are invariably lower than desktop virtualization, too.
- **VDI licenses:** VDI is an unquestionably powerful solution, however, it's also the most expensive. You should understand what your lowest viable number and highest affordable number of VDI licenses to understand how you're going to structure your

BYOD delivery estate. It is obviously beneficial to steer towards lower numbers of VDI licenses and it may be worthwhile to exercise some strict prioritization on which software to deliver through BYOD and who has access to it. A proof-of-concept or phased launch can also be highly valuable in making sure you can achieve your goals through BYOD whilst keeping it viable in a business capacity.

- **CALs for VDI style solutions:** Considered to be one of the most significant and unanticipated hidden costs of VDI are the CALs and VDA licenses required for launching apps through VDI, (CALs are required for server-based delivery of apps. VDA licenses are required for access to full virtual desktops). In order to access a single application, users must be delivered an entire desktop. For non-multisession VDI (All persistent VDI and some non-persistent) there must be a one-to-one ratio of desktops to users. Not only does this mean more VDI licenses, but also more Client Access Licenses to purchase. Consider solutions capable of multisession VDI to keep CALs and VDI license costs to a minimum. The newly-released Windows Virtual Desktop is a great example of this. [Windows Virtual Desktop capable of multisession Windows 10 and CALs are absorbed into its cost.](#)
- **VPN licenses:** In order to provide secure access to university systems and facilities, VPNs are advisable. Higher education IT must beware of malware and brute-force attacks, whether intentional from users or by secondary exposure to malware they and their machines have fallen victim to.

## Server Cost

- **Application virtualization servers:** Servers to store and host applications ready for virtualization are necessary and you will require enough hardware infrastructure to accommodate all the software titles you need to deliver. Unlike VDI, servers for application virtualization implementation are lightweight; that's because the applications just stream from those servers and actually run on the end-device.

- **VDI servers:** As VDI virtualizes a full desktop in order to deliver apps, the server infrastructure required is quite substantial. With this cost in addition to VDI license costs, you can see why it is beneficial to keep VDI use as low as possible.
- **License servers:** For applicable software titles, you may need license servers to contain and provide license keys and other forms of licenses for apps to call on and utilize for on-demand delivery. This will likely be more frequent for software delivered by application virtualization.
- **Storage servers:** With BYOD enabled, if users begin saving files locally (especially when launching apps through application virtualization) it may be that usage of storage servers decreases. However, they will still be required, and you can collect data throughout the process of implementing and providing BYOD to inform your decisions.

## Soft Cost

- **Support:** As previously mentioned, support may see some growth in demand initially, though once BYOD is implemented and your students are used to the user experience and how to access their software, the load on support will likely decline. This is one of the [key benefits of BYOD](#). You may see a shift in the nature of support requirements.
- **Specialist staff for maintenance:** Some aspects of the various technologies required for BYOD are very specialist. VDI as a whole requires significant specialist knowledge and application packaging will require someone familiar with and skilled in the practice. Application packaging can be outsourced in a scalable fashion, however, VDI maintenance and provisioning cannot.
- **Internal marketing and rollout:** A BYOD policy must be communicated to your staff and students and, in a sense, 'sold' to them. We've seen a trend of users (particularly faculty) being hesitant to accept change in how they access their software, so you will need to communicate the benefits of BYOD to them. Furthermore, you'll need to provide clear instructions on how to access their software and a clear route to support should it be required.

## Arrange your demo of AppsAnywhere

Schedule a one-to-one demo with one of our product experts to learn how AppsAnywhere has helped hundreds of universities deliver thousands of software titles to millions of students on their own devices, on and off-campus.

[ARRANGE YOUR DEMO](#)



**1.5m+**  
users



**15,000+**  
apps



**150+**  
universities



**1 awesome**  
student experience



## 4. How to get the most out of BYOD

## Communication to Users

BYOD carries with it a number of significant benefits, all of which can directly influence student experience, enrolment and retention, IT's assignment of budget, and ultimately, revenue. Ensuring your BYOD policy gains the maximum possible uptake is the route to accessing the following key benefits:

- Reduce specialist labs
- Reduce hardware investments
- Provide a better student experience and user experience
- Reduce software access support tickets
- Improve student outcomes, retention, and success

## Strong and consistent branding

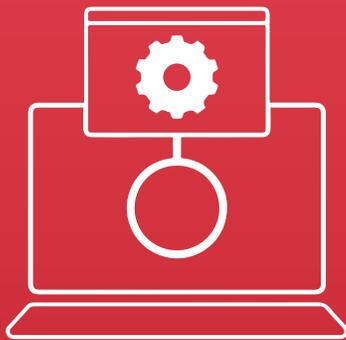
Just like any product or solution, giving your BYOD policy a name, brand and identity will help students and faculty identify it, gain familiarity with it, and generate some personal investment in it. Having a clearly signposted place that they get their software will have drive adoption and usage, and increase your student outcomes down the line.

## Digital marketing materials

Most universities with a BYOD policy will create at least one webpage of information and links regarding the policy. The webpage should be designed to rank in search engines alongside your university's name and should be easily locatable. Social media images/posts and alert dialogues on managed machines are a great way to communicate your BYOD policy with students and faculty.

## Physical marketing materials

Flyers and posters around campus have been known to really boost the use of BYOD policies. Distribute them in relevant locations and high traffic areas to create maximum exposure and inform your users that they can access university software on their personal machines.



# 5. Software Delivery Glossary

# Software2's Software Delivery Glossary

From thin clients to hypervisors, and from containers to kernels, software delivery is a complex subject, full of jargon and specialist knowledge! Read definitions of all of software delivery's technical terms and jargon, and get further insight into the technology behind virtualization solutions with Software2's comprehensive Software Delivery Glossary.

GLOSSARY



# Next steps to improving the way you deliver applications...

Get a personal walkthrough of how AppsAnywhere works from one of our product experts

Arrange a demo

Experience AppsAnywhere for yourself in our free, hands-on trial environment

Try it now

# Software2

software2.com