Cyber safety sorted

family zone | EDUCATION SOLUTIONS

WHITEPAPER

BYOD Responsibility in Schools

Where does a School's responsibility for BYOD begin and end?

family zone | EDUCATION SOLUTIONS

Contents

Introduction

This Whitepaper tackles the number one question for school managers implementing Bring Your Own Device (BYOD) programs: “how much responsibility rests with the school?”

Governments, school managers, teachers and parents recognise that the next generation of learners require access to online resources to facilitate engagement, collaboration, the development of higher order thinking skills and to give students valuable real-world experiences.

Digital literacy, including data literacy and coding skills, is required to equip this generation of students for the future of work in which exponential technologies feature significantly.

BYOD is a popular option for schools, putting the (often subsidised) cost of Chromebooks, laptops and tablets back on the parents. It is estimated children use three devices during their school years, not including smartphones. At the same time as schools are initiating 1:1 programs, school leaders and IT managers are very aware of the risks posed to school, staff and learners when student tablets, laptops and smartphones enter the classroom.

Be it inappropriate usage, classroom management issues, technical problems, theft and breakages or pressure on bandwidth, school leaders need to find a balance between empowering the learners and protecting the school, staff, parents and especially the students for whom they have a duty of care.

This Whitepaper advocates the approach of ‘All Care, No Responsibility.’ Schools adopting this approach are in the powerful position of being able to engage students in proactive ongoing discussion on how to use the internet, rather than resorting to reactive measures on inappropriate internet usage after the event.

family zone | EDUCATION SOLUTIONS

Student BYOD Device and obligations

A student BYOD device is not a school device, and as such the student will have definite obligations regarding the provision of and the condition of the laptop, tablet and/or smartphone. This rests solely with the student, not with the school, and comprises the basis for the 'No Responsibility' element of the approach.

The school's commitment will be for 'Care' of the environment in which the student will be using the tablet or laptop and in educating the student. This sits alongside the care and education provided by the home, and should be a partnership.

The duties of the student and school are expanded on below.

1. The student's obligations:

The student is responsible for keeping the device charged and in a sound working state. This should be made very clear from the beginning of the BYOD program via a school policy, information sessions and parent / student documentation. By making this clear, teachers can remain focused on teaching and will not be turned into IT technicians by proxy, distracted from their main objective of facilitating learning.

Students also need to comply with school internet use policies while on school grounds.

2. The school's role:

Schools are just as accountable for ensuring that students are safe in a virtual world as they are from a physical standpoint, and these obligations are often defined at government level. Many school BYOD programs stall due to concerns that the school cannot provide a safe online environment. Schools worry that they do not know what students are doing on the network and what content they are accessing.

This hesitation is warranted. A school's role within a BYOD program is to provide 'All Care' – a secure and safe environment. The school must be confident that inappropriate content is properly filtered and if people do something they shouldn't, that this is acted on in a proactive and positive manner. Should an incident occur, the school leadership team must have clear visibility around which students were involved, what the behaviour was and when it occurred. This information needs to be clear and easily accessible. The school can then address the issues through evidence-based conversations. This level of visibility over the devices and network is not only for the benefit of the student, but for management, staff and parents.

3. The Shared Role:

The school's role also extends to that of educating students to become safe, ethical and responsible digital citizens. This requires ongoing programs for the staff, students and the parent community. Parents and caregivers should feel empowered to become involved in their child's online world, instilling their values of how to behave and how to share and connect in a safe and responsible manner. Such regular school-to-parent communications, alongside increased parental access to their child's learning, can encourage parents to become more engaged and potentially lead to benefits in terms of student achievement.

Achieving ‘All Care, No Responsibility’

There are four factors required for a school to achieve ‘All Care, No Responsibility’. Firstly, a well-functioning and resilient infrastructure, secondly the technical ability to track individual usage, thirdly the development of a culture of transparency and accountability and finally, ensuring internet usage does not impede learning-related activities.

Well-functioning and Resilient Infrastructure

Teachers and students will be frustrated if teaching and learning is impeded by technical issues and bottlenecks on the network. The school requires a network management system with easy to manage policies and granular auditing to ensure that the backend runs smoothly.

Tracking Individual Usage

In order to be able to understand individual student internet use it is vital that the user of any school or BYOD device is identified. The technical name for this process is called ‘user authentication’. Without identifying the student, it is not possible to properly respond to inappropriate or distracted behaviour or be able to control how a device can be used within a class or throughout the school. By identifying the student using the device, personal internet usage can be recorded against their account. In addition, internet access can be filtered according to group membership, for example by year group, home class or collaborative team. Most networks have existing authentication systems to identify a user when they log into a Windows machine or use a shared Chromebook.

The same approach can be applied to a BYOD program. When a student brings any device onto the WiFi network they are asked to authenticate using their existing school account details. This approach can be achieved by choosing a network access management system that integrates directly with your existing network infrastructure. By choosing a system that augments your existing network with BYOD support, it is not necessary to spend substantial budget upgrading your existing network and wireless infrastructure. Once ‘user authentication’ is a given, all internet use is visible and a school can focus on establishing a culture of transparency and accountability.

> “Our openness reflects real life in the digital world and prepares students instead of shielding them.” – ALEX DAROUX, HEAD OF IT, TE AROHA COLLEGE

Establishing a culture of transparency and accountability

Historically the solution to managing internet access has been to restrict access to the handful of websites that the school has deemed to be learning-related. This approach is no longer tenable given the vast number of online resources that can benefit student learning.

> “With our existing system, we could not see what students were doing, we couldn’t easily monitor traffic on the network and we had instances of students using staff logins on their own devices and we needed to put a stop to that.” – JOHN TOPP, DEPUTY PRINCIPAL, PORIRUA COLLEGE

A combined technical and educational response is needed to operate a high-trust model of online behaviour in schools. In high-trust environments, inappropriate internet use can be addressed via tools that give teachers live visibility over student network use. Should inappropriate or off-task behaviour occur the teacher can then choose the best response given the individual student and the lesson context.

When students are aware that their internet use is visible to teachers and staff their online behaviour is more likely to align with the school's policy around appropriate internet use and network access privileges are respected. This transparency can also allow schools to educate students to the reasoning behind any internet access policies. For example, should a student be using a torrent site to stream movies they can be made aware of the issues around liability for this copyright infringing behaviour, and students who consume excessive amounts of data on non-educational resources can be made aware that such use will slow access to learning related activities for other students. Should a student continue to disregard their internet access agreement, an effective response is to reduce their personal internet access privileges and for their teacher or dean to have a discussion with them.

Responding to inappropriate use through visibility and conversation results in students aligning their behaviour with the school's agreed internet usage policy. This policy, and the procedures should the policy be infringed, should be circulated to parents, caregivers and students and signed agreements collated.

Ensuring internet usage does not impede learning-related activities

Having potentially thousands of devices connected to the network wirelessly can become a real drain on a school's resources. Difficulty logging in or slow internet access speeds will quickly frustrate students, who will soon stop lugging their devices around, and the BYOD program will ultimately fail.

Students streaming music or torrenting movies can slow your network to a crawl and impede learning related activities. To ensure that learning opportunities are not impeded by inappropriate network use, it is best to take a proactive approach to managing website and application usage through visibility and control. Having systems in place that enable reporting on network use allows schools to identify which non-education websites and applications are bandwidth hogs. It is also critical to be able to easily change network access and filtering policies so that the insight provided by understanding network use can be acted upon.

Schools should be able to easily self-manage these policies so that changes in network use can be responded to, whether that be blocking an application outright or only permitting access outside of lesson hours. Whilst these four factors will ensure that a school can achieve 'All Care, No Responsibility', they also lead to positive outcomes for other school stakeholders.

Positive Outcomes For Stakeholders

By choosing a network access management system that enables the above factors, all stakeholders (principals, teachers, students and parents) will benefit from the functionality provided.

Principals

Principals will be able to share their duty of care by delegating network management concerns to the relevant dean or staff member responsible for a given student's character education. Having timely notification of inappropriate usage enables the dean or equivalent to have appropriate conversations with students around internet use and guide students towards more responsible behaviour. Principals will also be able to ascertain how different parts of their digital ecosystem are being utilised. They can look at usage data for certain systems practice informed evidence-based decision making.

Teachers

For any BYOD programs to succeed it must have the support of the teachers. If a teacher does not feel comfortable or confident that BYOD devices are being used constructively then they will choose not to use them.

The visibility provided by the 'All Care, No Responsibility Approach' will give teachers access to tools that allow them to easily manage and align classroom internet access with lesson content. Teachers will see which students are off-task and can respond accordingly. When students are aware that their online behaviour is visible, it is also more likely to be learning focussed.

Teachers will also have control over classroom internet use. Should the school's default filtering policy be blocking access to a lesson relevant resource, teachers can override default behaviour to allow access to lesson appropriate content. Conversely, allowing teachers to restrict internet access for the current lesson to a defined list of resources can keep students within a 'walled garden' by preventing access to unrelated websites and applications and increasing focus and engagement in learning.

Often network systems are overly complex to administer and maintain, making it too hard or expensive to change access settings to meet the school's changing requirements. At other times, network systems block sites that are useful to learning. It is important that any network access management solution is easy to use for both administrators and teachers to ensure that network access policy is helping teachers to improve students' learning outcomes. The proper classroom internet management tools can make the difference between teachers embracing or forgoing the benefits these devices can offer. Placing visibility and control over classroom internet use in the teachers' hands increases the chance of BYOD devices being integrated into the classroom successfully.

Parents

When asking parents to furnish BYOD devices it is only fair that they have confidence that device usage will be well-managed, learning-focused and that access to inappropriate content will be prevented. Parents should be made aware of BYOD policies and school internet use policies too.

Students

Ultimately a BYOD program is all about improving student learning outcomes. A successfully integrated BYOD program that is fully utilised by teachers, supported and understood by parents and trusted by management will empower the learners to confidently and independently navigate the network and internet, as they would in the 'real world'.

The visibility and transparency made possible by the right network management system will set the learners up to be the digital citizens required for the careers of the future.

Summary

When supporting student devices on the school network it is critical to draw a clear line of responsibility between the school and the student. Doing so allows students to understand school BYOD expectations and staff to ensure that students are using these devices in a constructive and learning focused manner.

Choosing the right support tools and classroom control features can assist teachers in integrating these devices into their lesson plans, and enable schools to measure the success of their BYOD program.

About us

Linewize is a Family Zone company, with a shared vision of keeping students safe online on any device, any time.

Learn more

Visit us www linewize com, email us at info@linewize com, or call us +64 (0) 3 668 1218

Sources:

Childrens Internet Protection Act:
https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

The underutilized potential of teacher-to-parent communication: Evidence from a field experiment:
https://scholar.harvard.edu/mkraft/publications/underutilized-potential-teacher-parent-communication-evidence-field-experiment

family zone

www.familyzone.com

ABOUT US

Family Zone is passionate about making student internet management easy. We help school teachers ensure that student internet use is constructive and education focussed. Our tools work with existing networks to create an online environment that respects student agency whilst highlighting inappropriate use.

CONTACT US

New Zealand:
www.linewize.com
ph: 09 888 9285

Australia:
www.familyzone.com
ph: 1300 398 326

USA:
www.familyzone.com/us
ph: 844 SAFEWEB (844-723-3932)