Hybrid Learning checklist for IT admins

“ This checklist covers the key areas an IT admin must focus on to adopt a hybrid learning model in classrooms ”

ONBOARDING STUDENTS

- [ ] Are your students and teachers equipped with the necessary hybrid learning tools and technology?
- [ ] Have you enforced a streamlined way to deploy learning devices to staff and students?
- [ ] Have you set up user accounts and synchronized relevant data including course details, emails, class groups, and academic calendars?
- [ ] Have you ensured that students have 24/7 access to an uninterrupted internet connection?

MANAGING PRODUCTIVITY & COLLABORATION

- [ ] Do you record and maintain time and attendance reports for both online and face-to-face students?
- [ ] Have you set up collaboration tools to assist students and staff to achieve a hybrid learning environment?
- [ ] Do you have tools in place that enable both virtual and in-person students/staff to communicate with each other?

APPLICATION AND CONTENT MANAGEMENT

- [ ] Do you have tools in place to remotely deploy apps and content to institutional devices? (VPP, Apple Classroom, Schoolwork)
- [ ] Do you block students and staff from installing harmful or unproductive apps on institutional devices?
- [ ] If required, do you possess the ability to lock down devices to a specific set of apps or websites during school hours?

DATA PROTECTION

- [ ] Do you ensure that sensitive information of student/staff is kept confidential and secure?
- [ ] Have you made it mandatory to require a VPN to access your institution's apps and resources?
- [ ] Do you restrict students and teachers from accessing sensitive data via unprotected Wi-Fi networks?
- [ ] Have you blocked your students/staff from accessing suspicious apps and websites on institutional devices?
- [ ] Do your data protection policies comply with the regulatory guidelines in your region?
- [ ] If required, do you possess the ability to locate lost devices, lock them down, and in worst cases wipe the sensitive information stored in them?
- [ ] Are students and teachers educated in identifying phishing, social engineering, and other security threats online?

ENDPOINT SECURITY

- [ ] Do you enforce restrictions and security configurations on student/staff devices?
- [ ] Are student/staff devices updated to the latest patches and operating systems?
- [ ] Have you enforced encryption and password policies on institutional devices?
- [ ] Have you enabled firewall and installed antivirus software on student/staff devices?
- [ ] If required, do you possess the ability to automatically lockdown devices that wander outside the school area?
- [ ] Do you enforce BYOD policies for students and staff who use personal devices to access institutional resources?

IDENTITY AND ACCESS MANAGEMENT

- [ ] Do you maintain and update the list of students and staff who work both remotely and in-person?
- [ ] Do you restrict student/staff access to sensitive information such that only users with the right privileges may access and edit it?
- [ ] Do you authenticate students and staff with MFA/passwords/biometrics, before granting them access to the institution's apps and resources?
- [ ] Do you make use of tools such as SSO to streamline your authentication processes?

REMOTE MONITORING & TROUBLESHOOTING

- [ ] If required, do you possess the ability to remotely view and/or control the screen of institutional devices?
- [ ] Are you able to track the real-time location of institutional devices, and enable students and staff to check in with their location data?
- [ ] Can you remotely ring devices, see their location, and if necessary, power off/restart devices, and clear their passwords?
- [ ] Can you broadcast important messages to your managed devices?
- [ ] Can you remotely push scripts to your devices and automate time-consuming tasks such as creating folders, moving files, etc?

AUDITING & REPORTING

- [ ] Do you perform regular checks to verify that students and staff comply with institutional policies?
- [ ] Do you regularly monitor the health and status of institutional devices?
- [ ] Do you keep a record of the applications installed on institutional devices?
- [ ] Do you maintain and manage a history of the location details of institutional devices?
- [ ] Do you periodically review your security policies to identify weaknesses and potential vulnerabilities?