STEP 2
NEEDS
What are the technological components of a successful one-to-one initiative?

Implementing a successful one-to-one technology initiative requires more than simply acquiring a device for each student. At a minimum, districts will need the following: one-to-one devices, internet connectivity, device security, and a learning management system (LMS).

**One-to-One Devices**
One-to-one devices are the central component of any one-to-one initiative. These devices include tablets, laptops, or laptop-like devices such as Chromebooks. Some devices may require add-ons (such as keyboards for iPads) that do not come standard with the device as well as warranty and protection plans to cover the inevitable damage that will happen to some devices. (For more information about selecting and purchasing devices, see Step 4.)

**Internet Connectivity**
Another obvious component of a one-to-one initiative is internet access. While most schools already offer internet through a wifi connection, the sudden influx of hundreds or thousands of additional devices may require additional wired or wireless capacity. Districts implementing a one-to-one initiative will need to work with their internet provider to determine if wired capacity in each school building as well as wifi capacity within each building will be sufficient for the new demand. Districts also need to consider how to provide internet access to students outside of school hours, as almost half of Mississippi households (42%) lack access to high-speed internet. (See Step 5 for strategies to address this aspect of internet connectivity.)

**Device Security**
One often-overlooked component of implementing a one-to-one initiative is ensuring that there are security measures on all devices to protect personal data, filter online content, and monitor internet and application use. The need for many of these measures is enshrined in the federal Children's Internet Protection Act (CIPA). There are a few options for implementing necessary security measures. For an additional price, some educational technology vendors will offer to “pre-configure” devices with certain security measures in place. There are also a number of individual service providers that will work with districts after devices have been purchased to provide the tools necessary to ensure student safety and comply with federal law. Either way, the implementation of proper security measures is a critical step that must take place before students receive one-to-one devices. (See Step 4, Step 5, and Step 6 for more details.)

**Learning Management System**
A learning management system (LMS) is a platform in which whole schools or districts can operate on one streamlined system. It provides a centralized location for educators to develop and disseminate content and for students and their families to access everything from individual lessons and materials to grades and attendance information. While many districts in Mississippi already utilize a student information system (SIS) like PowerSchool to track grades, LMSs can be utilized to facilitate virtual learning. (See Step 5 for more details.)

In addition to generally addressing these four components, districts may want to conduct a more formalized needs assessment. Included in the Mississippi Department of Education’s (MDE) Digital Learning District Guidance is a Digital Learning Capacity Assessment, which districts may find useful for this purpose. In addition to the MDE guide, readers will find a capacity assessment, guiding questions, and next steps related to other areas. We will reference these resources when applicable throughout this toolkit.
What additional staff responsibilities will be necessary to implement and manage a successful one-to-one initiative?

Depending on the pre-existing capacity of each district, district technology staff will encounter varying “additional” responsibilities. For higher-capacity districts, implementing one-to-one will merely entail scaling up their current practices to accommodate additional devices. For districts less accustomed to utilizing digital learning tools, implementation may require an entirely new set of responsibilities for staff members. The extent of additional responsibilities will also depend on the size of a given district as well as the district’s specific goals. Consider the experiences of these two districts, one small and one large:

**Booneville School District**
Booneville, Mississippi

- **1,300 students**

When Booneville adopted its one-to-one initiative in 2012, Director of Technology Dustin Pounders remained the only full-time employee in the technology department while his responsibilities quickly multiplied. Before one-to-one, Mr. Pounders reported his role as primarily waiting for teachers to run into technology problems. Once implementation of one-to-one was underway, his new responsibilities began requiring him to work around the clock on a daily basis to manage the initiative. The reason for this shift was that Mr. Pounders had to start keeping up communication between himself, parents, and students. Handling calls, emails, inquiries, and repairs became a primary aspect of his role as Director of Technology. Booneville later hired one additional part-time staff member for its technology department to reduce the strain on Mr. Pounders, but he remains much busier than he was prior to one-to-one.

**Highline Public Schools**
Burien, Washington

- **18,000 students**

In a district as large as Highline Public Schools, it would be nearly impossible for one individual to handle maintaining a one-to-one initiative. Thankfully for Technology Director Mark Finstrom, his technology department staff consists of four primary staff members, not including himself, who divvy up the various responsibilities. One individual is responsible for application and third-party tool monitoring and operations; another oversees program development and provides ongoing support and training; one manages field technicians and device maintenance; and another is solely focused on expanding wireless internet connectivity—a specific goal of the district, which is of even more importance now with virtual learning.

In a larger district such as Highline Schools, allocating responsibilities among multiple technology staff members is crucial to the ongoing success of one-to-one.
Whether these responsibilities are new, and whether additional staff are required, districts should ensure that technology departments have the capacity to perform the following functions:

**One-time actions for the initial implementation of one-to-one**

### Developing a handbook and student/parent contracts:
Developing a handbook is necessary for making sure that expectations are clear from the beginning and for signaling compliance with applicable laws and regulations. This action should be carried out with the input of key stakeholders (e.g., teachers, administrators, etc.) and with a clear understanding of the law. For legal purposes, contracts must also be developed to signify acceptance of these policies by students and their parents. *(See Step 6 for more details.)*

### Expanding wifi access in and out of school:
Wireless internet access is essential for reaping the benefits of one-to-one. Without it, students are unable to access the wide array of resources that become available with successful implementation. Given the mass increase in the number of devices using a school’s wifi, wireless access must be expanded and updated regularly. Additionally, provisions should be made for students without wifi access at home (e.g., hotspots, wifi centers, etc.). *(See Step 5 for more details.)*

### Selecting and ordering devices:
Acquiring the devices for a one-to-one initiative requires a good deal of research into what type of device will best fit the needs of a district as well as how to get the best price on these products. Once a district selects the best device for its needs, staff will also need to obtain vendor quotes, examine bulk pricing discounts, and select the best vendor. *(See Step 4 for more details.)*

### Developing a plan to distribute devices to students:
Depending on the implementation plan (e.g., whole district, certain schools, certain grades, etc.), staff will have to determine the most efficient way to roll out devices. Generally, even if a district goes one-to-one all at once, in later years, when the devices are upgraded or switched, distribution is completed in a staggered fashion to ensure greater ease and lessen the financial burden. *(See Step 8 for more details.)*

### Selecting and implementing a learning management system:
A learning management system (LMS) is not absolutely necessary for one-to-one success, but it will be beneficial in promoting academic progress among all students while simultaneously allowing for the necessary instructional differentiation to take place. An LMS will be a particularly critical tool if virtual learning has become necessary. Similar to the selection of one-to-one devices, selecting and implementing an LMS will require a fair amount of research, which will involve directly reaching out to LMS providers about pricing and customization. *(See Step 4 and Step 5 for more details.)*

### Determining device security standards:
Administrators, as well as the technology department, should familiarize themselves with relevant laws and regulations, such as CIPA. Additionally, the department should develop a clear set of guidelines to ensure device security and disseminate these guidelines to students, teachers, and other staff to better protect themselves and the network. Along with this, administrators should determine which individuals will have access to different types of student data. *(See Step 5 and Step 6 for more details.)*

### Selecting and implementing filters:
A key aspect of ensuring student safety when accessing the internet involves setting up content and application filters. Most schools already do this on their existing wireless network, but it will need to be updated. With all students on the same wireless network, filters must be in place prior to the dissemination of devices. If you decide to purchase a security software system (such as GoGuardian or Securly), this filtering aspect can be achieved through that service. *(See Step 5 for more details.)*
Recurring actions for the ongoing management of one-to-one

Maintaining inventory of one-to-one devices: After investing hundreds of thousands of dollars to provide one-to-one devices to students, technology staff must keep track of these digital learning tools. This will include maintaining records of which devices have been provided to which students as well as ensuring that the remaining inventory of devices are prepared for distribution. Technology staff should keep track of new purchases and devices that need to be replaced.

Repairing devices: In addition to general technical support, districts will need intermittent repairs to one-to-one devices—either as a result of faulty hardware or student accidents. There are a few options for handling repairs: while some repairs may be handled in-house by the technology department (depending on the nature of the damage as well as the technical expertise of the technology staff), it is likely that many repairs will have to be outsourced to the technology vendor or another company that specializes in these repairs. Either way, districts should have a clear plan in place to handle repairs in a timely manner, which, at the very least, will require technology staff to coordinate with a third party. We also recommend that districts purchase warranties (three-year warranties are common), as this will cut down on costs related to this step.

Replacing devices: Districts will likely have to replace the devices every three to five years, so a conservative estimate requires that districts be prepared to replace on a three-year basis. In order to save money and ensure a smooth rollout, many districts use a staggered schedule, with different grades receiving new devices in alternating years, rather than replacing devices all at once.

Handling tech-related inquiries from students, parents, and teachers: Providing basic technical support will likely be one of the more time-consuming aspects of managing a one-to-one initiative, but with a clear, well-structured system in place to field inquiries—whether via email, over the phone, or in person—a district can save time and ensure that teachers and students take full advantage of educational technology. Some strategies for providing efficient technical support include setting up a specific phone number and email address for submitting inquiries directly to technology department staff or instituting a more decentralized system in which teachers take responsibility for fielding initial inquiries, with the option to refer students to the technology staff. Either way, it should be clear to students, teachers, parents, and technology department staff alike who is responsible for handling technical support inquiries as well as how to get in touch with them.

Determining what applications and websites need to be filtered: In addition to carrying out this action upon the initial implementation of one-to-one, content and application filters must be updated regularly, as websites and applications shift and change every moment. In many cases, a bi-weekly or monthly update should be enough to maintain the necessary filters.
The Children’s Internet Protection Act, or CIPA for short, was first enacted by Congress in 2000 and requires that schools receiving discounts through the E-rate program restrict access to certain content on the internet that may be deemed obscene or harmful to minors. The Federal Communications Commission (FCC) requires certain policies to be in place in order to abide by CIPA, including those outlining how the online presence and activities of students will be monitored and how students will be informed of appropriate online behavior. (See Step 6 for more information on policies.)

The protections required by CIPA are the minimum—districts will almost certainly need more device security than required—but each district/school must follow CIPA guidelines to be in accordance with the law and eligible for the E-rate program. Regardless of whether a school or district is eligible for, or participates in, the program, understanding CIPA is a good place to start when it comes to assessing current or future device security measures. While technology staff should be well-versed in the implementation of filters to abide by CIPA, districts can generally opt for educational technology vendors to "pre-configure" devices, at an additional cost, so that they are CIPA-compliant upon arrival from the vendor. Visit the Federal Communications Commission’s webpage on CIPA to learn more about the law and its requirements.