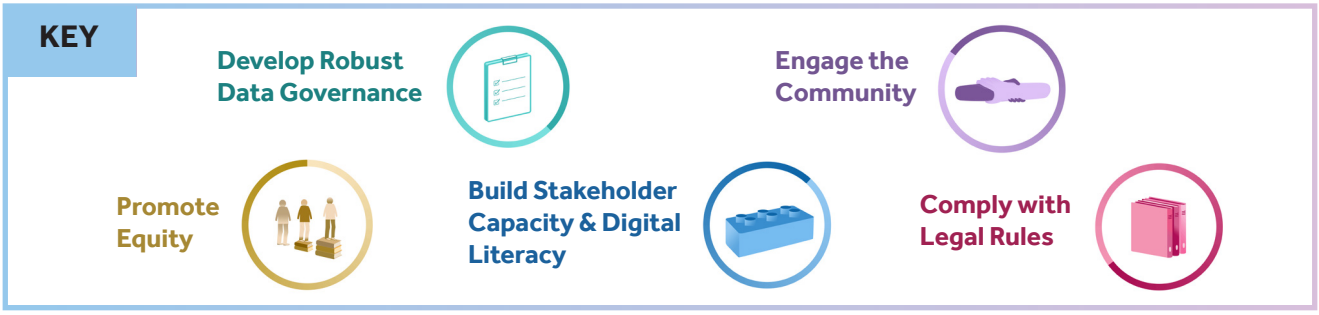
Checklist: Transitioning to Connected In-Person Learning

Returning to in-person learning will likely not look and feel the same as it was prior to the pandemic. COVID-19 continues to present a risk to students' and families' health, schools are responding to renewed calls for equitable learning, and widespread distribution of devices, educational technology, and broadband connections have created new opportunities – and risks – for students, families, and educators. The steps below will help schools meet those changes and challenges while protecting student privacy and promoting equity.

KEY



Establish or Update Data Governance Procedures

- ☐ Update existing data governance procedures and structures to include new or expanded uses of data and technology that resulted from the pandemic (like videoconferencing software, school-issued devices such as hotspots or tablets, and new data collections like COVID-19 vaccination information).
- ☐ Review data sharing agreements for compliance with legal requirements and best practices, and to ensure they reflect the planned uses of online learning services once students are attending school in-person.
- ☐ As part of data governance, provide a mechanism to hear from parents and community members to ensure that decisions reflect their concerns and meet their needs.
  - ☐ Include topics such as feedback on what was effective, what was not, and **what services marginalized groups (such as students with disabilities) would like to retain.**

Train Stakeholders on Integrating Technology Into Classrooms and Safely Using Technology

- ☐ Proactively communicate with parents and students on technology that will be used in the classroom, the data it is using, and how the data will be protected.
- ☐ Train educators on how to safely and securely use technology, including how to navigate security and privacy settings.
- ☐ Offer training, resources, and technical support for families to ensure they can resolve any issues with new technology without compromising security and privacy.
- ☐ Provide training to educators on how to ensure that the benefits of data and technology are available to all students, such as by accommodating students who lack broadband access at home or who require accessibility equipment.
- ☐ Avoid using technology to create "tiers" of learning opportunities (such as by using online learning for the long-term suspension of students).

Checklist: Transitioning to Connected In-Person Learning

Apply Data Minimization and Privacy/Security Best Practices to Data Collection and Sharing Needs

- ☐ Adhere to data minimization principles, secure collection and storage techniques, and privacy protection practices when collecting data, including as required by the U.S. Department of Education under the American Rescue Plan.
- ☐ Adopt best practices for sharing data with health agencies and other partners, including secure methods of transfer and entering into data sharing agreements.
- ☐ Comply with legal requirements for sharing data with health agencies, including the requirements of the health and safety emergency exception under FERPA.
- ☐ Employ secure collection and storage techniques.
  - ☐ Utilize encrypted transfer and storage methods and avoid insecure methods (such as email or fax).
  - ☐ Develop access controls (such as password protections and user permissions) to ensure that only employees with a "need to know" may access student data.
  - ☐ Determine whether and how the data will be integrated with existing systems (such as student information systems).
- ☐ Avoid inequitable results from technology meant to monitor for COVID-19 by accounting for the invasiveness, effectiveness, cost, and potential discriminatory effects of certain technologies, especially on students of color and students with disabilities.

Disclose Data to the Public on Learning and COVID

- ☐ Adhere to best practices for disclosure avoidance to ensure that individual students are not identifiable in released data.
- ☐ Comply with legal requirements for disclosure avoidance.

Checklist: Transitioning to Connected In-Person Learning

Resources

- Jessica Li, Center for Democracy & Technology, *Sharing Student Health Data with Health Agencies*: https://cdt.org/insights/sharing-student-health-data-with-health-agencies-considerations-and-recommendations/
- Jack Becker, Center for Democracy & Technology, *Commercial Companies and FERPA's School Official Exception*: https://cdt.org/insights/commercial-companies-and-ferpas-school-official-exception-a-survey-of-privacy-policies/
- Cody Venzke, Center for Democracy & Technology, *Student Privacy, Transparency, and COVID-19*: https://cdt.org/insights/student-privacy-transparency-and-covid-19/
- Student Privacy Policy Office, U.S. Department of Education, *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service*: https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service
- Student Privacy Policy Office, U.S. Department of Education, *FERPA and the Coronavirus Disease 2019 (COVID-19)*: https://studentprivacy.ed.gov/resources/ferpa-and-coronavirus-disease-2019-covid-19
- Privacy Technical Assistance Center, U.S. Department of Education, *Data De-identification: An Overview of Basic Terms*: https://studentprivacy.ed.gov/resources/data-de-identification-overview-basic-terms