AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175
www.riaclu.org
info@riaclu.org

April 10, 2020

Superintendent Michael Messore
Barrington Public Schools
283 County Road
PO Box 95
Barrington, RI 02806

VIA MAIL AND EMAIL

Dear Superintendent Messore,

In the wake of the recent, and indefinite, school closures in Rhode Island, emergency steps have appropriately been taken to accommodate remote learning for all public school students. Since school-loaned devices, such as Chromebooks, and third-party programs that facilitate online learning are being used for virtual education in most districts, we are writing to ask – if you have not already done so – that you take prompt action to protect the privacy rights of students and families making use of these devices and platforms.

The ACLU of Rhode Island has, for several years, expressed concerns about school district policies that give officials broad and fairly indiscriminate abilities to remotely access school-loaned devices while in students' hands at home. It is additionally of importance to note the substantial invasions of privacy that can occur when third-party programs are installed on personal family computers as well. For example, a program like Go Guardian – which we understand is being used by some school districts – not only provides real-time access to a student's computer, but can allow school personnel to examine weeks of web history and data on the computer, which could include the private browsing history of the student's parents. The emergency transition to fully remote education heightens the acute need for districts to take steps to preserve student privacy in both of these capacities.

When the ACLU of RI surveyed school districts three years ago on their policies governing home use of such devices, we were troubled to find that almost every district authorized wholesale access to the laptop's content – including files, photos, and web history – at any time and for any reason, even when families were encouraged to use the computers for non-academic purposes. Even more ominously, the authorization rarely barred school access to, and activation of, the device's microphone and camera.

In February of this year, as you know, we filed a follow-up open records request to determine if those policies had changed at all in order to provide students and their families with much-needed privacy protections. Although your district has yet to respond to this most recent request, the response to our inquiry from 2017 revealed that the policies for such programs for Barrington Public Schools indicated that students should have no expectation of privacy, that the district maintains the right to remote access of the device, and that the school retains the right to inspect the device at any time and for any reason.

Although we did not inquire into whether your district utilizes remote teaching platforms such as Go Guardian – and we recognize that any usage of such platforms may only be in response to the current closures and public health crisis – it is additionally important for your district to disable any features that intrusively authorize access to information beyond what is necessary for classwork.

Given the ongoing nature of the school closures, and the need to balance both the administration of reliable educational services and the maintenance of student privacy while classes are conducted outside of school, we therefore urge you to immediately adopt privacy protections regarding at-home computer use, and make students and parents aware of those protections. They should include the following:

- An outright prohibition on school officials' ability to access the microphone or camera of a school-loaned device except during live teaching activities and with the student and family's full knowledge.
- A ban on accessing the data on a school-loaned device unless (1) a parent or guardian has signed a valid opt-in agreement which allows access by the district to specific and explicitly specified data, or (2) a school official has reasonable suspicion that a student has violated school policy, and data on the device contains evidence of the suspected violation.
- A restriction on remotely tracking the location of a school-loaned device without cause.
- Disabling privacy-invasive features on any third-party programs that students are required to download in order to participate in virtual learning.
- Ensuring that any third-party programs used in the course of remote education are in compliance with the state's data-cloud computing privacy law, §16-104-1.

Since the implementation of school-loaned device programs, the ACLU of RI has been approached by many parents who felt uncomfortable with signing away their child's privacy rights but were given no other option for engagement in the important educational activities taking place with them. Now that students, and their parents and guardians, have no other option but to continue their education through such devices – and, on occasion, utilize their home computers for this learning – we believe it is imperative that the privacy rights of students be protected. Clear standards on access to the visual and audio components of the computers – whether school-loaned or personal – are essential. Also of tantamount importance is ensuring that platforms such as Go Guardian do not expose sensitive information about students and their families to school staff, and that the usage of such platforms does not unintentionally facilitate the ability for school staff to access more data than they need to complete their job responsibilities.

We hope that you agree, and we ask that you advise us of any action you plan to take to address these consequential privacy concerns. The ACLU of Rhode Island would be happy to assist in the drafting of procedures or policies that promote this important goal, and we look forward to hearing back from you. Thank you for your consideration.

Sincerely,

Steven Brown
Executive Director

Hannah Stern
Policy Associate