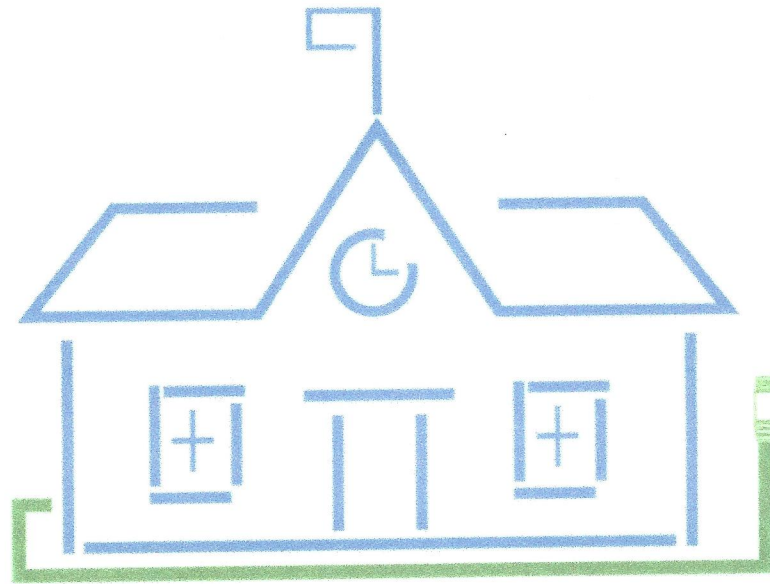




TechSafeSchools

Mitigation Techniques for Reducing RF Radiation in Classrooms

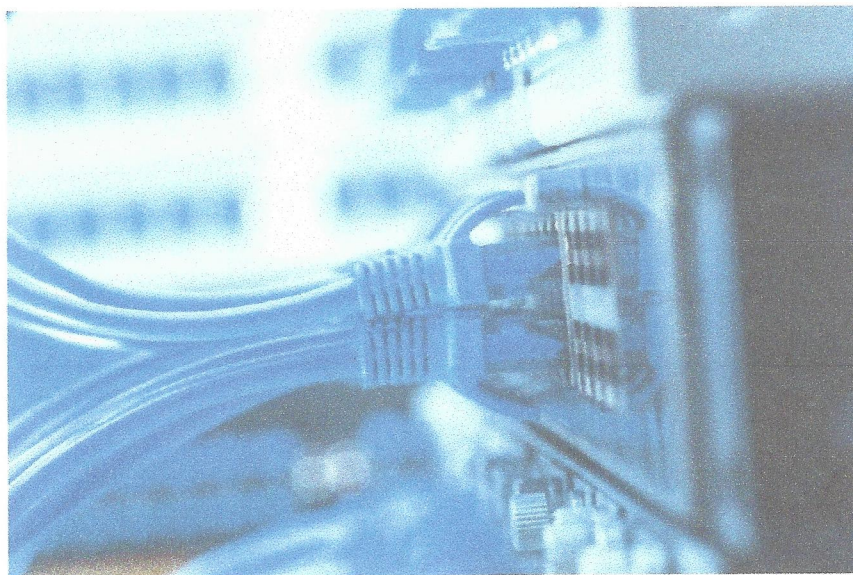
This document is part of a comprehensive web-based program to raise awareness about the potential harm of RF microwave radiation in classrooms, advise schools of potential legal liability for inaction, and to provide school administrators and technical personnel with simple steps that can be taken to reduce radiation exposures. For more information please visit www.TechSafeSchools.org

Introduction

Over the past several decades, scientists have discovered how the human body can be impacted by exposure to radiofrequency (RF) radiation, and how the developing bodies of children are particularly vulnerable. A recent (2018) study by the National Toxicology Program of the U. S. National Institutes of Health found “clear evidence” of cancer from exposure to this type of radiation - a finding that disproved the theory that non-ionizing radiation is harmless, which was the basis for all government regulations for more than 40 years.

This puts school administrators in a difficult spot. Many schools have invested heavily in wireless technology, having been repeatedly assured by the purveyors of wireless systems that their equipment meets or exceeds all government safety guidelines. Now we know that those guidelines are based on a disproven scientific theory. The question now is, ***what should we be doing about it?***

The TechSafe Schools program is designed for those school administrators who believe in the *Precautionary Principle* when it comes to our children, and in making wise and informed decisions to protect their schools from legal liability. In these pages we present some simple strategies for reducing RF radiation in classrooms as a temporary measure until all school systems can be hardwired.



(1) <https://www.niehs.nih.gov/news/newsroom/releases/2018/november1/index.cfm>

Measuring RF Radiation

The following mitigation techniques are designed to help you reduce exposure to “As Low As Reasonably Achievable” (ALARA). Before adopting any of these mitigation techniques, it’s critical to know and understand what kind of exposures currently exist.

We recommend a consultation with a professional who is trained in measuring RF exposures. The typical cost for this professional service is \$1,200 to \$2,000. We do not generally recommend asking tech vendors to perform this testing due to obvious conflicts of interest and lack of professional training.

As an alternative, school IT personnel can purchase or rent a professional grade RF meter to test exposures. There is a huge variation in the quality and reliability of meters used to conduct RF surveys. We strongly recommend one of the following meters to obtain accurate and meaningful measurements:

Safe and Sound Pro II

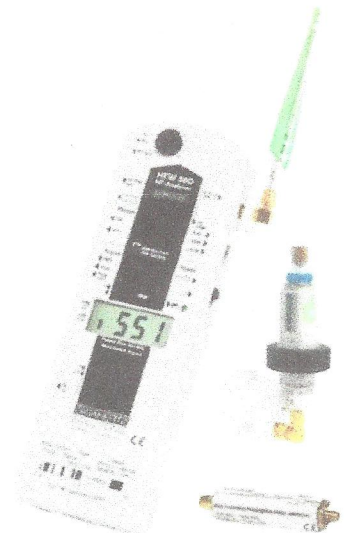
- Accurately reads both bands of Wi-Fi and cellular phones
- Rigorously tested in a lab, with published frequency response
- +/- 6dB accuracy from 400 MHz to 7.2 GHz; verified by a third party.
- Can detect signals from 200MHz to 8GHZ.
- **\$385 USD**

Acoustimeter (AM11)

- 200 – 8,000 MHz ± 6 dB ± 0.02 V/m
- **\$385 USD**

HFW59D Plus RF Meter Kit

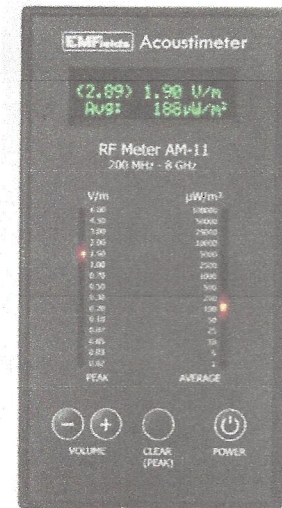
- Most accurate meter to measure Wi-Fi but will not measure most cellular signals.
- Most accurate, but costs more.
- 2.4 GHZ to 10 GHZ @ +/- 4.5dB
- **\$1200 USD**



For a more detailed explanation of meters and how to take readings, please view the TechSafeSchools webinar “Technical Forum on Reducing Wireless Radiation in Schools” on theTechSafeSchools.org website.

Basic Meter Operating Protocol

1. Wave the meter in figure 8 pattern while slowly rotating 360 degrees so that your body doesn't block any signal.
2. Keep the meter >1 foot away from metal, mirrors, or other reflective surfaces and all wireless devices.
3. Measure the average and peak (maximum) exposures and record data (V/m uW/m²)



Baseline Measurements - Step By Step

1. Turn off, unplug or disable all wireless devices, including wireless access points and smart boards.
2. Remove or power down all laptops, tablets, computers, cell phones, wearables, Bluetooth speakers and other wireless devices as these may still be transmitting, even if they are in standby or airplane mode.
3. Ensure all wireless devices and personal devices are off in neighboring classrooms including those located above, below or beside the classroom being measured.

Getting the Data

Obtaining accurate measurements of RF radiation in a classroom is not a simple task. Readings (and radiation exposure) can be affected by building materials, the presence of metal or other reflective objects, the number of devices in use, etc. Please view the webinar for more details.

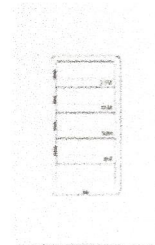
Peak vs. Average Exposures

The parameter used by the FCC to determine exposure limitations for humans is time-averaged Specific Absorption Rate (SAR). However, time-averaging is not how the body experiences the effects of RF radiation. In fact, this measurement method actually obscures the unique characteristics of intensity-modulated (pulsed) RF radiation that many scientists believe is responsible for causing biological harm.

Time & Distance

Reducing Wi-Fi Availability

Classroom exposure to RF radiation can be reduced significantly by using Wi-Fi only on demand, and only for a specific pedagogical curriculum where connectivity to the internet is required and hardwiring is not available.



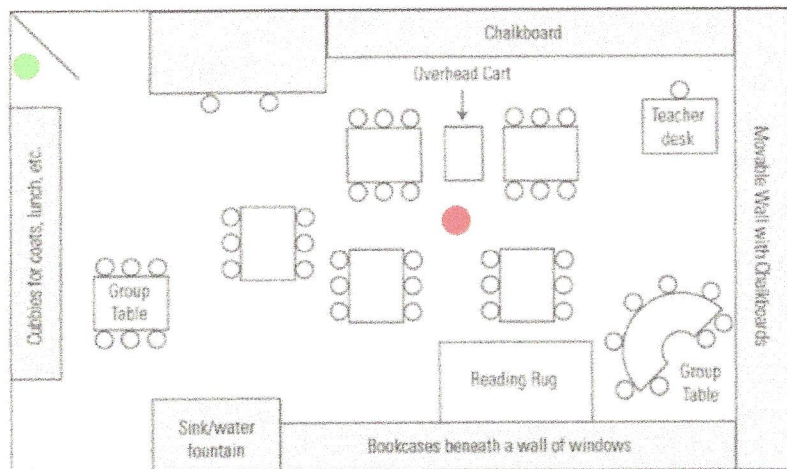
The simplest and most effective method of limiting the availability of Wi-Fi is to control the power to the wireless access points by means of a wall-mounted timer switch. The switch should be wired to control a dedicated outlet providing power to the routers and wireless access points in the local network.

Cost: Approx. \$175 - \$250 per classroom.

Increasing Distance

The amount of radiation exposure a student receives from routers or wireless access points decreases with distance. Every time the distance from a source to a child is doubled, exposure is reduced by 4X, or 400%.

One of the easiest ways to reduce proximate exposures for students is to locate the router or wireless access point in a distant corner of the classroom, away from student desks or tables. In most cases this will have no observable effect on device performance.

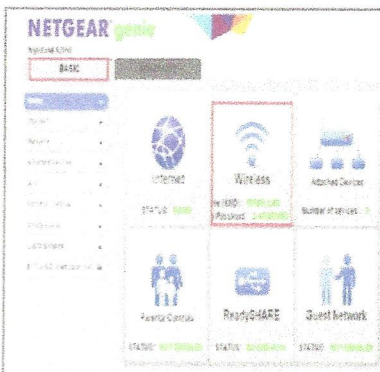


Depending on the layout of the classroom, the area above the main entry door is usually free from desks and student activities.

Reducing Power and Beacon Frequency

By default, most routers and wireless access points are set at the factory for full power to ensure maximum performance and coverage. Most schools use "enterprise wi-fi," designed to connect hundreds of devices with each router or wireless access point capable of providing coverage for spaces up to 2,000 square feet, far exceeding the amount of power needed for a typical classroom situation.

Fortunately, adjusting the power for most systems is a simple software adjustment.

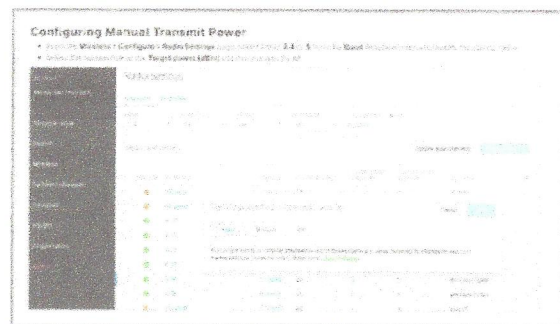


You can access the power output setting for Netgear's equipment using its online portal. By default, Transmit Power Control is set to 100% on both the 2.4GHz and 5 GHz radios. For networks with a separate wireless access point in each classroom, the transmit power can be reduced to 25% or less without affecting connectivity to devices. The end result is much lower RF exposure in the classroom and surprisingly, many schools have found that performance actually increases in the wireless network due to greatly reduced interference between wireless access points.

A second adjustment to power that can reduce exposure is limiting which of the two commonly found radios (2.4GHz and 5GHz) are enabled. If you have a wireless access point in every classroom, disabling the 2.4GHz and keeping only the 5GHz radio active will reduce the RF exposure in the classroom even further.

Cisco's Meraki wireless access points are easily adjusted from the online interface. Select "Target Power," adjust settings and "Save." Again, make sure you make the adjustment for both 2.4GHz and 5.0 GHz radios.

These are just two examples of wireless equipment that can be adjusted to reduce exposure.

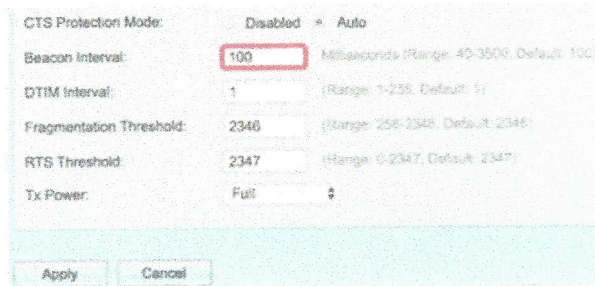


Contact your IT vendor for more information about making adjustments to your school's system.

Reducing Exposure Through Beacon Signal Adjustment

Beacon signals from routers or wireless access points provide connected devices with information such as SSID, timestamps, and various other parameters. Like the power output, the time interval between beacon signals can be easily adjusted. The higher the value, the more time between signals, and the less exposure for students and staff.

Most routers and wireless access points default to a beacon signal interval time of 100 ms, but this can be adjusted to a significantly higher number (e.g., 1000 ms) without impacting school environments, since most beacon signals are set to accommodate people moving around and shifting from one wireless access point to another.



The screenshot shows a configuration page for a wireless router. The 'Beacon Interval' is set to 100 milliseconds, which is highlighted with a red box. Other settings include CTS Protection Mode (Disabled), DTIM Interval (1), Fragmentation Threshold (2346), RTS Threshold (2347), and Tx Power (Full). The page has 'Apply' and 'Cancel' buttons at the bottom.

CTS Protection Mode:	Disabled	Auto
Beacon Interval:	100	Milliseconds (Range: 40-3500, Default: 100)
DTIM Interval:	1	(Range: 1-255, Default: 1)
Fragmentation Threshold:	2346	(Range: 256-2346, Default: 2346)
RTS Threshold:	2347	(Range: 0-2347, Default: 2347)
Tx Power:	Full	

Apply Cancel

Increasing the beacon signal interval can also significantly increase battery life. Again, testing is the best way to determine the proper beacon signal for your school environment.

Interval	Tx Power	Expected Range	Expected Battery Life *
100ms	3 (-12 dBm)	35 m (115')	Up to 7 months
300ms (default)	3 (-12 dBm)	55 m (115')	Up to 2 years
1000ms or 1s	3 (-12 dBm)	55 m (115')	Up to 4 years

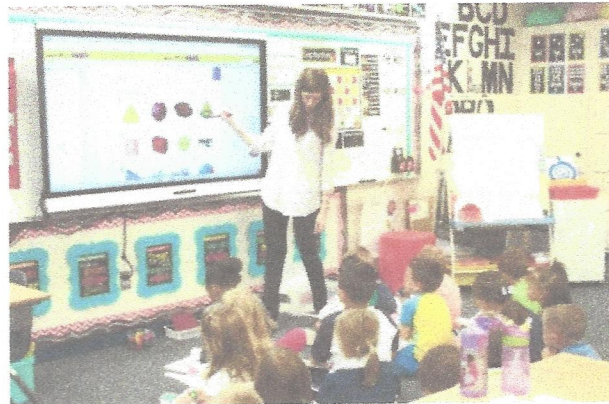
Please note: Reducing the levels of RF radiation through these measures is an important, but temporary step in mitigating exposure, and should not be considered sufficient to alleviate the problem or extinguish potential liability. We strongly advocate for the replacement of all classroom wireless technology with hardwired systems.

Hardwiring Options

Hardwired ("wired") classrooms are the safest and most secure learning environments for children. Wired systems are faster, more reliable, easily adaptable to new technologies and have none of the potential health issues that are becoming apparent with wireless technology.

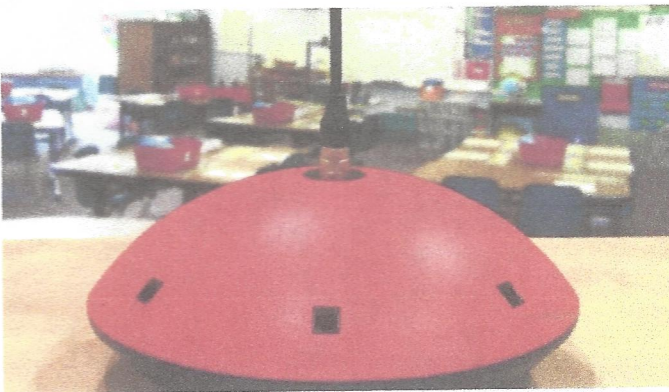
Wireless technology often requires frequent software upgrades, and over time, these costs can easily exceed the slightly higher upfront costs that may be associated with wired classrooms.

Start with some of the stationary devices such as smart boards, stationary computers and permanently-mounted cameras, and even more portable items such as projectors.



This may require the installation of a simple and inexpensive Ethernet switch to increase the number of available Ethernet ports in the room.

Ethernet switches come in a variety of configurations and can also carry Power Over Ethernet (POE) to provide power to wireless devices. Check manufacturer's specifications for more information.



Virtually any computer, smart phone, tablet or other similar device can be easily connected to the internet using simple, low-cost adapters.

Whether your school is using chrome books, iPads, notebooks or other devices, there are plenty of solutions to help students connect to the internet safely and securely.