All About Cookies:
Whenever you visit a web page, your browser requests many different files, fonts, html, images, style sheets and scripts that make up the page so that the page may be displayed to you. Some of these requests are fulfilled by the web site you are attempting to view, and some are fulfilled by one or more third-party sites working in conjunction with the site your browser is trying to display to you. As you browse the site, some of the files, scripts and other information that is requested might place cookies on your device.

There are different types of cookies, used for different purposes. In the broadest terms, we can break cookies down into 2 overarching categories:

- “Functional cookies” are often set so that a site is able to identify you and your device. There are a variety of reasons why this may be useful. For example, cookies allow the site to recognize that you are logged in, maintain your account preferences, or save what you have in your shopping cart until you check out.
- “Tracking cookies” are typically used by third parties operating on a site. They are there to follow or “track” the user across unrelated sites, services and sometimes devices. The information they gather can be linked to individual users and can be maintained over time. This is what happens behind the scenes when you visit a site to look at a product and then for weeks afterward you see ads for that product everywhere you go online. Tracking cookies are most commonly used for advertising and marketing purposes.

Cookies are the most common form of tracking technology, but many other tracking technologies exist, including web beacons, local storage, canvas and device fingerprinting. Each can have different privacy implications.

Privacy and Tracking Technologies
Any technology that collects data has implications for privacy. What those implications are varies depending on whether or not the tracking technology is used for functional or advertising purposes, how the technology is embedded into the site and on what pages. In some cases, the technology may be there to ensure that the website operates properly, and in other cases it may be something that presents legal issues when used on pages that are intended for students.

In addition, the security and privacy of trackers can also depend on how the service is configured. For example one of the most familiar forms of tracker are social widgets, such as the Facebook “Like” button and Twitter “Tweet” button. These offer a convenient way to share a site content. However, when a school adds social buttons to their site (or adopts service that does), depending on how the social media button was embedded and configured, they may be enabling those social media sites to track their visitors.
Create an Organizational Policy For Embedded Content

You might think that only the people that work with code need to worry about what trackers are in use on your district’s sites, but remember that trackers are called when content is loaded from an external source, so if your Content Management System, LMS or other applications allows embedding videos or other content from a third party site, there is the potential that this content may bring that site’s trackers along. Consider creating a list of what your internal content publishers are allowed to embed and when there are privacy implications or when required by those third parties, list those third-parties in your privacy policy with links to their privacy policies.

Follow Good Practices for use of Google Analytics in Schools

Google Analytics is one of the most prevalent measurement and analytics services, in use in 70% of the top 1 million websites. It can provide information on a website’s or app’s visitors, including number of unique and repeat visitors, referring sites, most frequent pages visited, what browser a visitor is using, ISP speed, and average time spent on a site or app. For a school system, this information can inform a decision to shift to a mobile-first strategy or (along with ISP speed) indicate requirements when adopting educational technologies, or aid in understanding the effectiveness of a district’s communication strategy.

As a good practice, and particularly where there is the potential for the use of a site or mobile app by students, school systems should:

- Be aware of their Google Analytics settings and follow any required conditions and disclosure in your website privacy policies, and consider providing users with information on how to opt-out of Google Analytics;
- Never send personally identifiable information (such as names, social security numbers, email, or similar data) to Google Analytics;
- Consider implementing Google Analytics’ IP Address masking feature. (Some Content Management Systems may only provide the ability to configure Google Analytics by adding the Google Analytics property ID, limiting the ability to enable setting such as IP Masking);
- Carefully evaluate the use of Google Analytics on pages where users provide information (e.g. forms), paying special attention to pages that pass sensitive information via the URL;

Provide Clear Privacy Policy Disclosures

Once you have an understanding of the services in use and the personal information being collected, ensure that your school or district website privacy policy discloses the presence of tracking technologies that are implicated in collection of personal information, as well as any required disclosures from third parties that may be operating on your site.

Perform a Privacy Inventory of Your District’s Tracking Footprint

One way to get a handle on your district’s use of trackers is to conduct a regular audit of major instructional and administrative systems, as well as your district website. An Excel worksheet with common categories of School systems can be downloaded from CoSN here.

For a more information on these topics, see the CoSN Member Exclusive Briefs