Life without Flash

You may be at risk of losing online resources if they use Adobe Flash.

Adobe Flash is used by web browsers such as Internet Explorer to display content like videos, animations and games. It runs in the background of your computer so there is a strong chance you are using it without even realising.

Flash has had security issues for years, such as a vulnerability in 2016 that could allow an attacker to take control of the affected system. This security issue was updated with a ‘patch’ but problems have kept occurring.

Adobe has announced that they will phase out Flash Player by the end of 2020, so if your online teaching resources use Flash Player, you are at risk of losing them.

Using Flash in teaching spaces.

As a result of these security issues, the university is transitioning away from Flash, so you may already have experienced trouble using Flash based resources. You can find more information on the IS ‘Click to Play’ blog post here: https://blogs.kent.ac.uk/isnews/clicktoplay/.

If you need to use a resource in a teaching space that uses Flash there is a strong possibility that it won’t work due to the way the Internet Explorer and Chrome now handle Flash content. Your best bet may be to test out the resource on a Student PC such as those in the Templeman library, Eliot and Rutherford or in the Drill Hall library on the Medway Campus, you can find PC availability here: https://www.kent.ac.uk/student/studying/pcrooms/. If you do so, you should test the resource using Edge (the web browser that comes with Windows 10). For the foreseeable future, Chrome will be available on the university PCs but we would recommend using Edge because it will be slower to phase out Flash support and current bugs in Google Chrome. It may be worth trying multiple browsers if you are having difficulty getting a resource to work.

How do I find out if my resources use Flash?

If you suspect a resource uses Flash, you can simply right-click what you believe to be Flash content and see if a Flash context menu appears, which looks something like this:

If you are using a browser which blocks Flash content, you may find an icon which looks like this:
What is the alternative?

An alternative solution called HTML5 is available which is supported by companies such as Microsoft, YouTube and Google. It works with the same multimedia elements as Flash but without all of the security issues. Many web developers have already begun moving across to HTML5, this means that it comes built in to most of the big-name browsers, so you won’t need to install anything extra.

A number of web browsers, including Google Chrome and Firefox, have begun blocking Flash; if a user wants to use Flash on these browsers they will have to click and reactivate them providing they trust the source. More details on how to do this for Chrome and Internet Explorer can be found on the ‘Click to Play’ IS blog post above.

What should I do about my resources that use flash?

If you manage a blog, web content or e-learning that includes Flash content, please find an alternative.

If you are unsure if a resource uses Flash, please contact helpdesk@kent.ac.uk.

If it does use Flash, please ask the content provider if they can offer an alternative such as HTML5, or find an alternative source for the content that does not use Flash.

Should I uninstall Flash from my home computer?

Not right away, as long as you keep it up to date to ensure your computer is safe. Some websites may not work if you uninstall it completely, some services can only be delivered via Flash. This will mean, however, that some resources that use Flash will work at home, but may not at the university. The safest way to use it is on a browser like Chrome which blocks the Flash elements until you verify they are safe. If you use Internet Explorer, you can turn on ActiveX Filtering to block the content in the same way.

To do so you can go to Settings > Safety > ActiveX Filtering as shown below.

When you have a site you trust, just click on the caution sign in the URL box and click Turn off ActiveX Filtering.