Managing your digital footprint

What is a digital footprint?

Every time you post, comment, or interact online you leave a digital footprint.

Your digital footprint is the data trail left by your interactions in the digital world. It's a public record of:

- what you said.
- what was said about you.
- what you liked, interacted with, or shared.
- where you are or have been.

Although it's less public, there's also a record of:

- what you've clicked on.
- what you've searched for.
- your IP address.

This guide is designed to help you manage your digital footprint and understand why it is important.

Why is it important to be in control of your digital footprint?

Your digital footprint becomes part of your online identity and what people see of you when they search for you online. Employers can, and do, trace your digital footprint on the internet when you apply for jobs with them. Often checking social media sites to see what type of content you are posting/engaging with so it's important to consider how that may look to an employer.

It is also possible for criminals to gather personal information about you to fraudulently impersonate you – things like applying for credit cards or gaining access to sites or systems in your name.

Websites you visit place cookies on your computer to allow advertisers to target you with products based on your browsing history. It's surprisingly easy to publish information about you online. Even if you aren't in the public eye, at some point someone might want to gather information about you with the intention of discrediting you.

How to manage your digital footprint

While it can feel overwhelming, the best thing you can do is become more aware and take steps to get some control over your digital footprint. The following steps are simple and effective, but you do need to set a chunk of time aside and be methodical in your approach.

1. Tidy up after yourself!

- Start by looking yourself up on the internet. Log out of your browser if you have an account, and then search for your name and usernames – where necessary in "speech marks" to get an exact match. Look through each page of results, until you're sure there are no more about you.
- Repeat the search with other browsers (Google Chrome, Microsoft Edge, Mozilla Firefox, Opera or Safari etc.). This process can take a while depending on how common your name is, but it's worth it.
- If you find something you'd like removed, you can usually ask sites directly to do this. You're quite likely to find that your name, address, county court judgements and more appear in online directories, particularly if you have appeared on an electoral register. (Been in court for failure to pay council tax? It might be an isolated incident, but that information could do you harm).
- Search social media sites directly (there's more about this in step 3).
- Get rid of old accounts you no longer use (and may have forgotten about). Consider whether it's appropriate for the public to see the musings of your 15-year-old self.
- There's lots of guidance about this online. Search for "how to clean your digital footprint" or "tools that help track your digital footprint". Be aware that some sites offer services to do this for you, but at a cost.

2. Don't rely on privacy settings

- First, understand that using privacy settings can only protect you so much. Friends, acquaintances, or others who have permission to see your pages can still download your pictures and repost them elsewhere, and comments can be retweeted or shared without your permission – either in fun, in error, or maliciously. So, if there's something you don't want to lose control of, don't put it in the public domain – even privately.

- Secondly, privacy settings change regularly. Check them often.

- Finally, don't include any private information (phone number or address) on your profile. Even information like your birthdate, place of work or pet names can be used against you for social engineering and identity fraud. Take care when using location-based sites like Foursquare or where you can tag your location (i.e. Facebook and Instagram). Don't announce when you're on holiday (and leaving your home empty).

- For more guidance, visit getsafeonline.org

3. Consider how you come across to others

- Review your activity on your accounts and identify anything that doesn't reflect you in anything other than a good light. Do the same for any other sites you may have used (including Q&A, chat, forum, and discussion sites), again, for all your usernames and accounts. It's important that you're impartial when you do this. You need to think about how you come across, consider how others might perceive your actions, and make any changes needed.

- Imagine the reaction of a future employer reviewing your posts to get an impression of you – and get rid of anything that doesn't portray you in a good light. Consider your chosen profession – for some you may need to be extra cautious and consider how things might easily be taken out of context.

4. Plan to stay in control

- Repeat steps 1, 2 and 3 every six months. Done regularly, it won't take nearly so long, but will help you stay in control.

- Next, and just as importantly, get strategic. Really think about your use of social media. How can it help you? Where does it fit into your life, and what can it help you do better?

- Read the guide 'Using social media for learning'. It'll help you become strategic and establish a personal code to ensure that your social media use is responsible.