3. Consider how you come across to others.

Look online for freely available tools that can identify which of your posts, tweets and images on Facebook and Twitter may be potentially damaging. Check all your accounts, and weed out those that don'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 to do this. You need to think about how you come across, whether you're negative, always seen with a drink in your hand, whether you are as witty and entertaining as you think you are, or whether you come across as a know-all, opinionated, boring, or with an axe to grind. Do you take pleasure in telling others they are wrong without constructive suggestions? 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 our leaflet 'Using social media for learning'. It'll help you become strategic and establish a personal code to ensure that your social media use is as watertight as possible in the future.

Get more advice

There's more help at **go.shu.ac.uk/socialmedia** including ideas for using social media for learning and how to use social media responsibly.

This leaflet was last updated in October 2014.

3969.3-10/14

Sheffield Hallam University

Managing your digital footprint

Four ways to stop your social media past damaging your real-life future

Managing your digital footprint

We tend to think of social media like real life. We have a conversation or a thought and then move on – forgetting that in the digital world a copy could be kept forever, unless we take steps to remove it.

This leaflet explains how to minimise any potential damage your previous use of social media might do to your future.

What is 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, retweeted 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 leaflet introduces four steps to taking control. For each one we've included suggestions for where to find more guidance, but there's plenty more advice online if you search for it.

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

Employers can, and do, Google people who apply for jobs with them. They could check social media sites that appear in the search to see whether you're the kind of person they want working for them.

Criminals gather 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.

And 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.

To find out more about why it's important, and about how information about you is used and shared, search for the Internet Society's resources on managing your identity.

Four steps to managing 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 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 Googling yourself. Log out of Google if you have an account, and then search for your name and user names – 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, Internet Explorer, Mozilla Firefox, Opera or Safari). 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 (such as Myspace or Bebo). Consider whether it's really 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 of all, understand that using privacy settings doesn't protect you. 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 – like your 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. Search online for 'examples of social engineering' for more on this. Take care when using location-based sites like Foursquare. And don't announce when you're on holiday (and leaving your home empty).

For more guidance, visit **getsafeonline.org**