

My Digital Footprint Campaign Kit



© CROWN COPYRIGHT 2015 | MY DIGITAL FOOTPRINT | CAMPAIGN KIT



National Protective
Security Authority

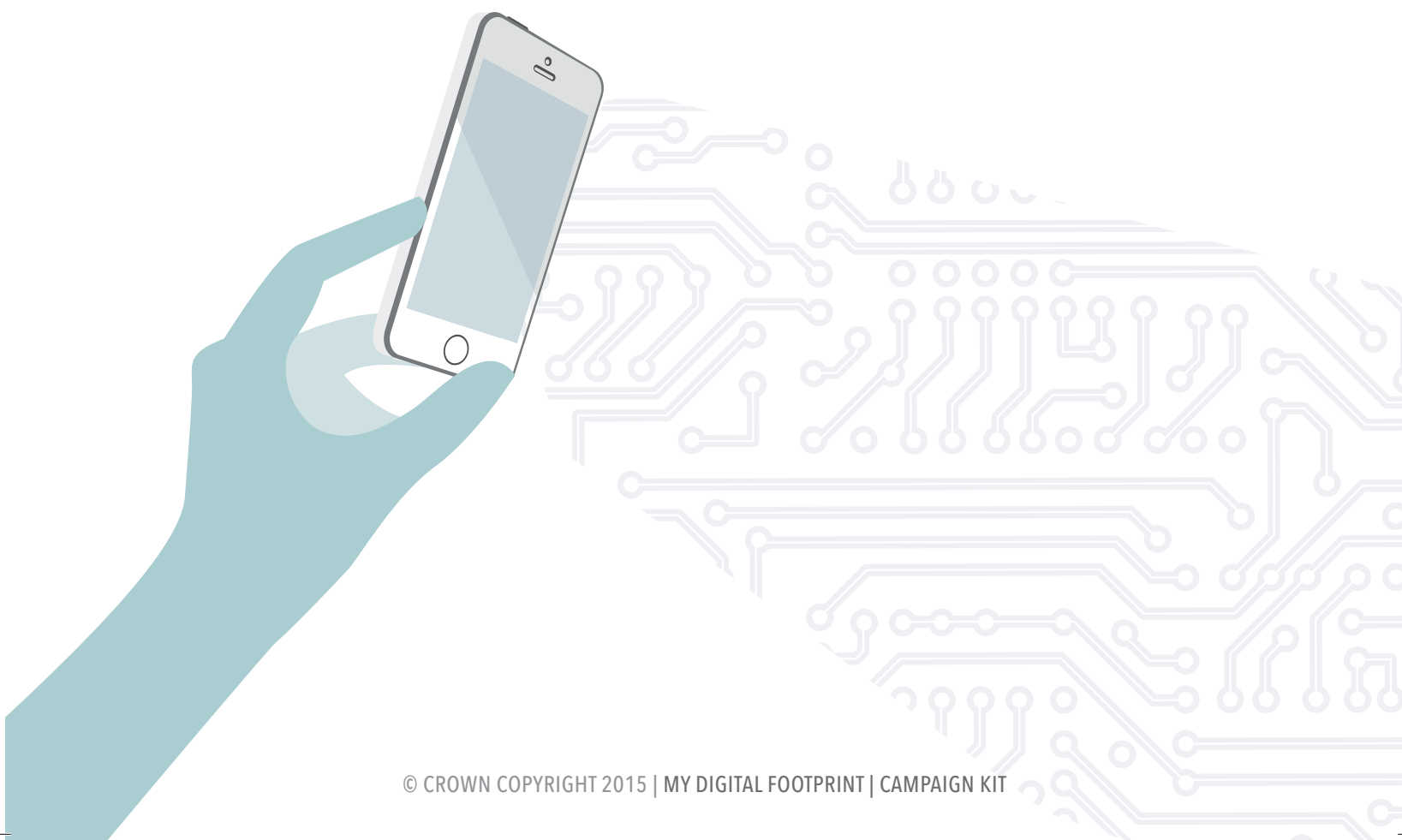


DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by NPSA. The views and opinions of authors expressed within this document shall not be used for advertising or product-endorsement purposes.

To the fullest extent permitted by law, NPSA accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

© Crown Copyright 2015. No content may be copied, reproduced, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted or distributed in any way (including 'mirroring') to any other computer, server, website or other medium for publication or distribution or for any commercial enterprise, without NPSA's express prior written consent.





INTRODUCTION

This campaign kit is designed to help individual staff members within the UK Critical National Infrastructure (CNI) ensure that they understand what their digital footprint looks like, how to manage and monitor it, and what impact it could have on them, their colleagues and their organisation if they fail to do so.

Of course, every organisation will have different expectations for how they'd like their staff to behave, depending on what's specifically at risk. But if you're stretched for resources, this easy-to-use kit offers practical security advice that everyone can follow, and the materials you need to run a campaign.

The campaign aims to deliver behaviour change by encouraging staff to do three things in relation to their digital footprint:

1. **Own it** – Know what your digital footprint looks like; know what information is out there about you, your family and the organisation you work for, and who else is posting about you online.
2. **Shape it** – Be proactive and shape your digital footprint into something you and your organisation are happy with; keep up to date with security policy and think carefully about what you share – you don't know who's looking at it.
3. **Monitor it** – Keep an eye on your digital footprint on a regular basis; social media privacy settings change, the devices you use change and the information about you online changes as you and others add to it.



PLANNING





The campaign materials in this kit are centred on the three principles listed on the previous page. They encourage staff to take individual ownership for their digital footprint and to manage this sensibly in light of where they work, the role they have and the threats they face.

This kit will help you communicate to your employees why their digital footprint matters, provide tips on how they should manage their digital footprint, and raise awareness of the consequences for them, their colleagues and the organisation if they don't.

DEFINE YOUR GOALS

Preparing a security campaign that aims to improve employees' security behaviours online should start by identifying how employees currently behave, and what needs to change in order for them to be more secure.

Begin by carrying out a behaviour 'audit' to give you an idea of where your employees are now and where you'd like them to be. **Ask yourself:**

-  How much do our staff use digital devices and services in their personal lives? For example, do you know what percentage of your workforce access social networking sites daily? Do you know what percentage have smart phones? And how many reference their place of work on their social networking profiles?
-  How often do staff use digital devices and services for work-related reasons? Do they use corporate or personal devices? Do they share personal details about themselves in relation to their work online, such as blogging or tweeting in their own name on behalf of the organisation?
-  What are the security threats and risks associated with your staff using digital devices and services? Could they make themselves more vulnerable to attack by linking their place of work with personal details about themselves online? Are some staff more vulnerable than others?
-  What is the organisation's risk threshold in relation to staff digital footprints? For example, are you comfortable if staff openly reveal online where they work and what they do, or is there certain information that should never be shared? What about staff use of personal devices for work-related reasons? Furthermore, what about where staff use their own digital devices in the workplace?



How would you like staff to behave when using digital devices and services in order to mitigate the security threats and risks to them, their colleagues and the organisation? Are these behaviours and standards clearly laid out in your security policies and procedures? To what extent do staff adhere to these currently?

Once you have the answers to some or all of these questions, you can begin to plan a digital-footprint security-behaviour campaign for your organisation, setting some clear goals. This could be as simple as raising staff awareness of their digital footprint through to encouraging staff to regularly review it and to take protective action accordingly.

Even if employees already follow your security procedures and guidance effectively, you can still use this kit as a reminder to keep it up.

GET BUY-IN

After defining your goals, the next step is getting buy-in from key stakeholders. These could include:

- **Senior management**
- **IT and/or information security**
- **Corporate communications, marketing and/or HR**

Senior management need to be committed to requiring good security behaviour and to changing behaviour that falls short. They can positively influence line managers who in turn communicate key messages to employees.

Your IT department and/or information security team may have some helpful suggestions regarding the content of your campaign.

Find out who can help communicate the campaign to staff. If you do not have a dedicated corporate communications team, then marketing and/or HR departments can often design and manage internal communications. They can help you reach your desired audience via various channels, such as:

- **Electronic** – e.g. email and intranet
- **Print** – e.g. posters or desk drops
- **Face-to-face meetings**



CREATE A PROJECT PLAN

Next, develop a clear and detailed project plan to enable you to record and track how you to intend to manage the running of the campaign.

You should think about:

Creation of a project team, including project manager

Clarification of the aims of the campaign

When the campaign will have the most impact

The time of the year

When to deliver each element of the campaign

Whether all the elements of the campaign are relevant to all staff

What other campaigns might be running, and whether this campaign could potentially conflict with or indeed support them

What other messaging is being given to staff (particularly in relation to social media use and the use of digital devices for work)

Other demands from within the organisation

How to measure the campaign's impact

When to refresh the campaign

Whether you can embed the campaign into long-standing packages such as inductions or security training





MONITOR

Finally, the ability to review and amend your campaign is very important, to identify the parts that work, and those that don't. There's no point in sending out a message that your staff just ignore.

After the materials have been up for a while, it's a good idea to evaluate how well they are working. Speak to members of staff, who will give you a good sense of how visible the materials are and whether they have changed their behaviour as a result.

You could do this by conducting a short questionnaire. This can help you assess whether your materials have been seen and if they have had an impact. A couple of tips to remember:

- A wider sample of recipients will allow an organisation to draw more meaningful conclusions.
- You can combine a numerical or quantitative element (e.g. "Yes / No", or "Agree / Neutral / Disagree" questions that can be turned into a percentage), with subjective or qualitative elements, which seek more general opinions.





MATERIALS IN THIS KIT

Listed below are the various materials included within the NPSA 'My Digital Footprint' campaign kit that you can use to help deliver your security campaign:

- **8 posters in A3 and A4 size, covering the following topics:**
 - Knowing what your digital footprint is
 - Considering how your friends, family and colleagues add to your digital footprint
 - Using separate email addresses for different online activities
 - Being careful about what you store on your devices
 - Knowing your IMEI number
 - Thinking about who you link up with online and how much you know about them
 - Thinking about how you share personal and work-related details online and about where this information is going
 - Remembering that once you share something online it is there forever

To see previews of the posters in the campaign kit, please see Annex.

- **Two digital footprint guidance documents:**
 - 'My Digital Footprint – A Brief Guide': This is a short introductory booklet for staff on what their digital footprint is, why it matters and the importance of managing it proactively.
 - 'Tracking My Digital Footprint – A Guide to Digital Footprint Discovery and Management': This is a detailed booklet for staff containing tips on how to find out what their digital footprint is and what they can do to minimise their vulnerability to some of the threats and risks.

ANNEX



Please note: The posters can be edited so you can include your organisational logo instead of the NPSA logo (Crown Copyright must be retained) and you can amend the text on where to go for further guidance.

LINKS

For additional information, visit:

- National Protective Security Authority (NPSA): www.npsa.gov.uk
- Get Safe Online www.getsafeonline.org

