# GETTING THE BASICS RIGHT

CPNI

Centre for the Protection of National Infrastructure

# 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 CPNI. 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, CPNI 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.

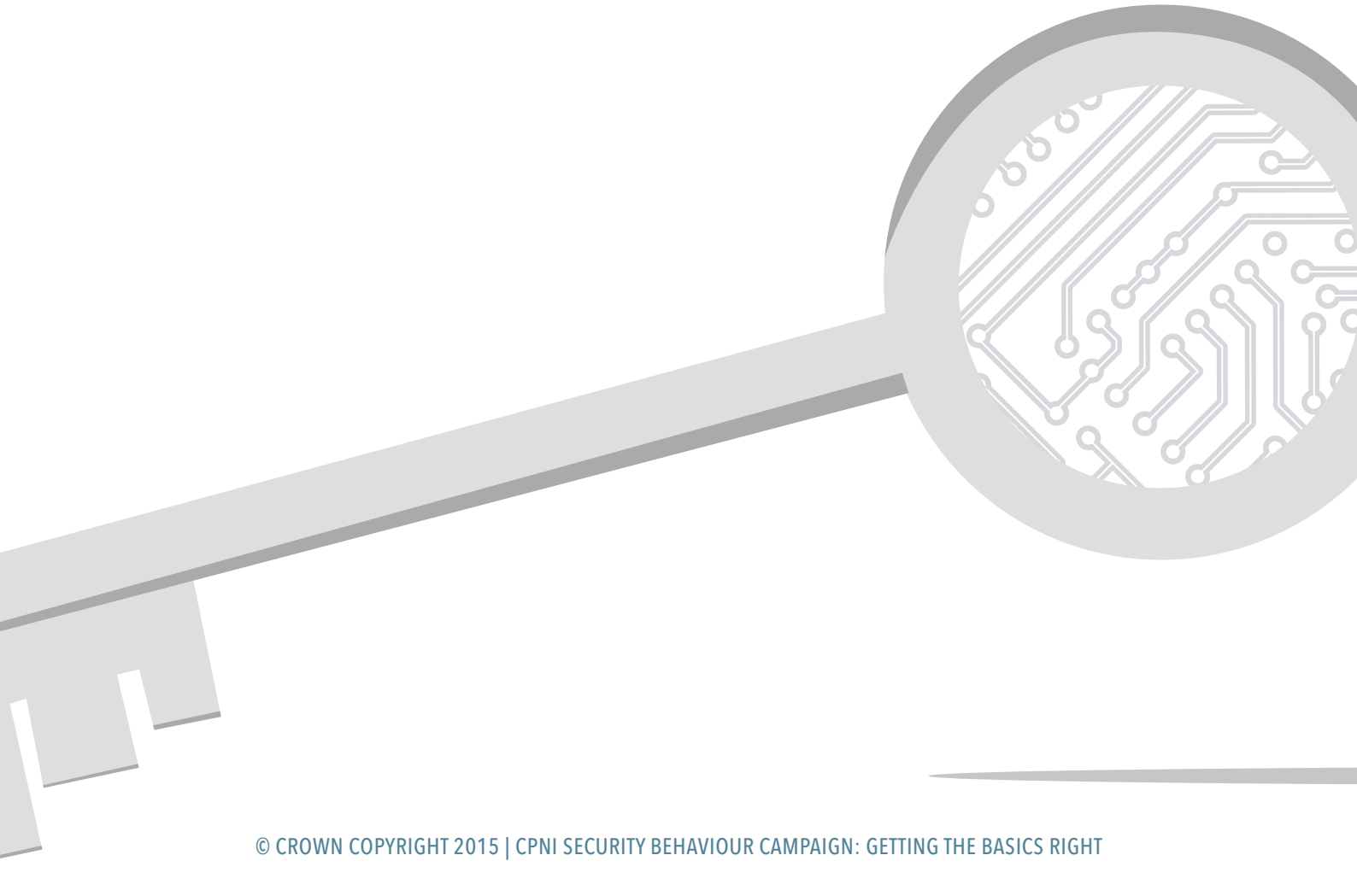
# INTRODUCTION

**This campaign** kit is designed to help individual staff members ensure that they are getting the security basics right, in and around the workplace.

Of course, different organisations expect staff to behave in different ways, 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 all the materials you need to run a campaign.

It addresses seven key issues. These are:

- Staff not wearing their pass while in the office or forgetting to take it off when they leave work
- Computers left unlocked when staff are away from their desks
- Staff continuing sensitive discussions outside the meeting room
- Sensitive documents being left out for anyone passing by to see
- Sensitive materials being destroyed inappropriately, such as not using a shredder
- Staff ignoring company security policies and measures
- Letting visitors walk around the office unescorted or without a pass



# PLANNING

**This kit** will help you communicate desired employee behaviours in and around the workplace, the reasons why certain security behaviours are important and how employees can work together to prevent lapses from occurring.

## DEFINE YOUR GOALS

**Preparing a** security campaign that aims to improve people's behaviours in and around the workplace should start by identifying how people currently behave, and what needs to change in order to be more secure.

Begin by carrying out a behaviour 'audit' to give you an idea of where you are and where you're headed. Ask yourself:

- What information and/or assets need to be kept safe in the workplace?
- What are the biggest security risks and threats you face?
- Do employees currently behave in a security-conscious manner in the workplace?
- Which key security procedures are frequently followed and which are not by staff?
- Are the security policies and procedures you expect staff to adhere to in the workplace clear, succinct and understandable?

Once you have the answers to these questions, you can begin to plan a security behaviour campaign. It all starts with keeping your staff aware of and updated on your official security policy.

And if your staff already follow security policies and procedures, use this kit to promote that good behaviour; remind them to stay the course and keep up the good work.

## GET BUY-IN

**Key to** your campaign hitting the ground running is getting buy-in from:

- Senior management
- Key departments that can help, such as corporate communications, marketing and/or HR

Senior management need to be committed to changing security behaviour from the outset. They can positively influence line managers who in turn communicate key messages to employees, so getting security issues to regularly feature in management meetings is very important.

Meanwhile, 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.

Get whoever is in charge of internal communications on board straight away and find out how they get their messages out to staff. 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

**Developing a** clear and detailed project plan will enable you to record and track how you intend to manage the running of the kit.

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
- What other messaging is being given to staff
- Other demands from within the company
- 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

**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 people 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:

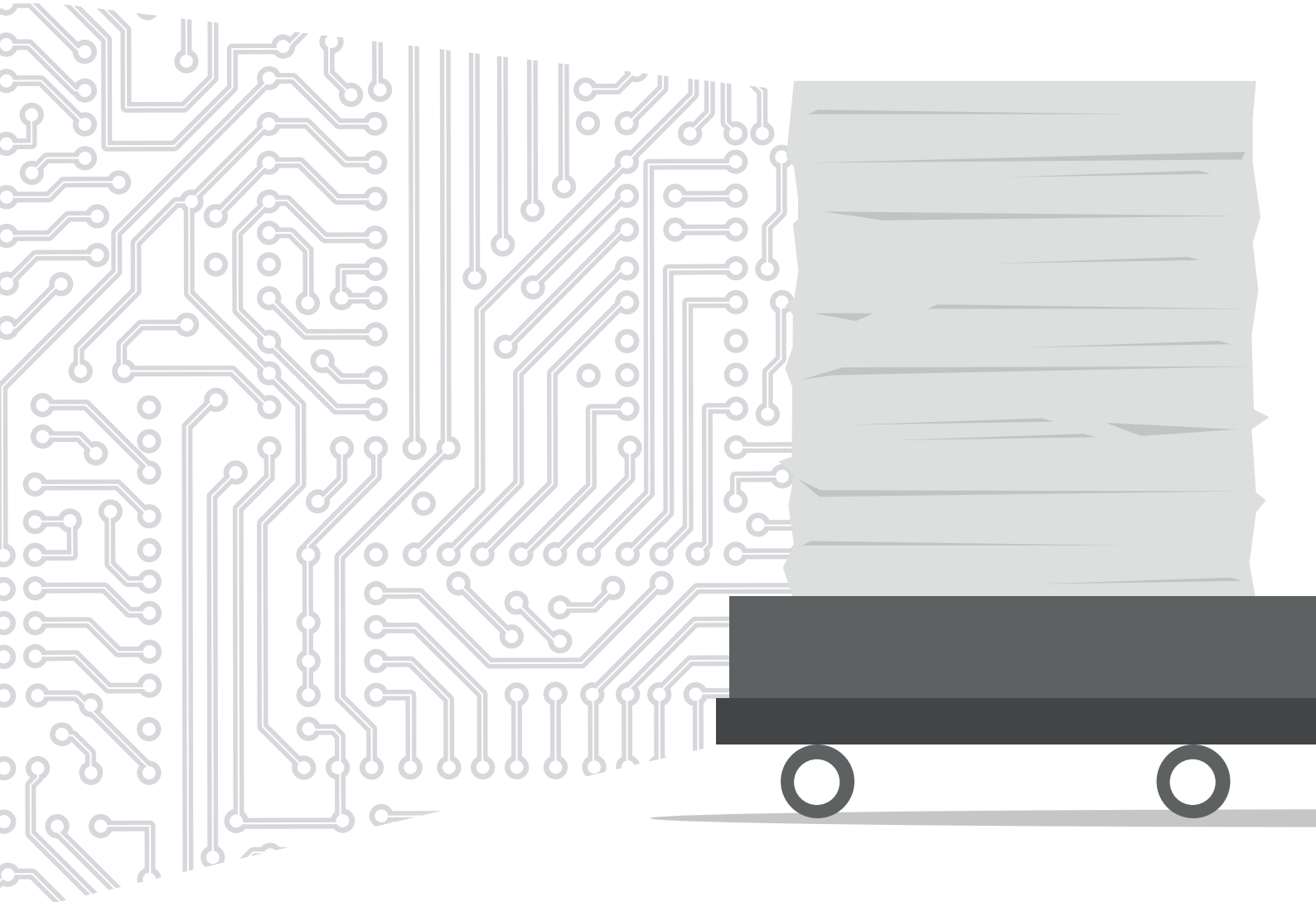
- A wider sample of recipients will allow an organisation to draw more meaningful conclusions.
- You can combine a numerical or quantitative element (e.g. "Yes or No" questions that can be turned into a percentage), with subjective or qualitative elements, which seek more general opinions.

# MATERIALS IN THIS PACK

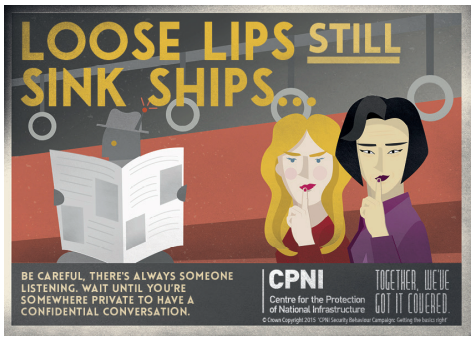
Visit **www.cpni.gov.uk/advice/personnel-security1** to access the range of materials that accompany this kit, which you can use to help drive your security campaign. These are:

- 12 posters in A3 and A4 size
- Three checklists: 'Workmate Bingo', 'Everyday in the Life', and 'Watch It!'
- One video: 'Getting the basics right'
- Downloadable graphics:
    - > A picture of all the posters individually in a 'sticker' format
    - > Computer wallpaper

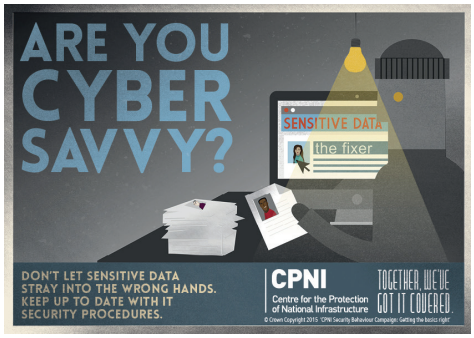
You can customise these materials to allow you to include a logo that is specific to your organisation or department.



# POSTERS



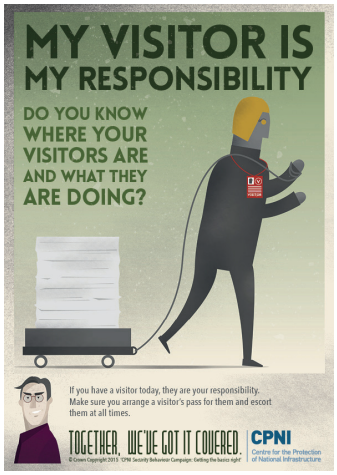















# VIDEO


Visit the CPNI website and CPNI YouTube channel to watch our new video "Introduction to Security: Getting the Basics Right".

# CHECKLIST GUIDANCE

## CHECKLIST 1 – WORKMATE BINGO

**In order** to encourage staff members to be on the lookout for security lapses by their colleagues, they might like to play 'Workmate Bingo'. Staff members are issued with a 3x3 grid 'bingo card' of unwanted security behaviours, which they compete to fill out.

The aim of the game is to get a 'bingo' by spotting the full list of potential security lapses listed below.

The company should determine the prize, though in an ideal world none of these cards would ever be completed, as employees would be encouraged to continue adhering to security policy, and not lose. Of course, you might also want to reward staff that manage to keep a completely clean scorecard!

All staff are issued with a scorecard, which they're encouraged to keep in a prominent position on their desks to encourage others to do the same. A staff member can stamp his or her bingo scorecard ONLY when:

1. They spot a colleague not following a security procedure
2. They point it out to that colleague or their manager

## CHECKLIST 2 – EVERYDAY IN THE LIFE

**Display this** chronological checklist like a poster on all employees' workstations to act as a 'desk aid'. It will ensure that employees are constantly reminded to employ best security practice at every point in their working day.

The design resembles an actual checklist with a 'tick-box' graphic next to each line, to remind the employee to make mental 'checks' as they go about their days.

## CHECKLIST 3 – WATCH IT!

**This is** a more general checklist. It serves more as a stylised department-wide poster that is meant to be posted in a prominent position where everyone can see it, as a 'quick-glance' reminder for employees to adhere to best security practice.

# LINKS

For additional information, visit:

- Centre for the Protection of National Infrastructure (CPNI): www.cpni.gov.uk
- National Counter Terrorism Security Office (NaCTSO): www.nactso.gov.uk

# THANK YOU

GETTING THE BASICS RIGHT

CPNI
Centre for the Protection of National Infrastructure