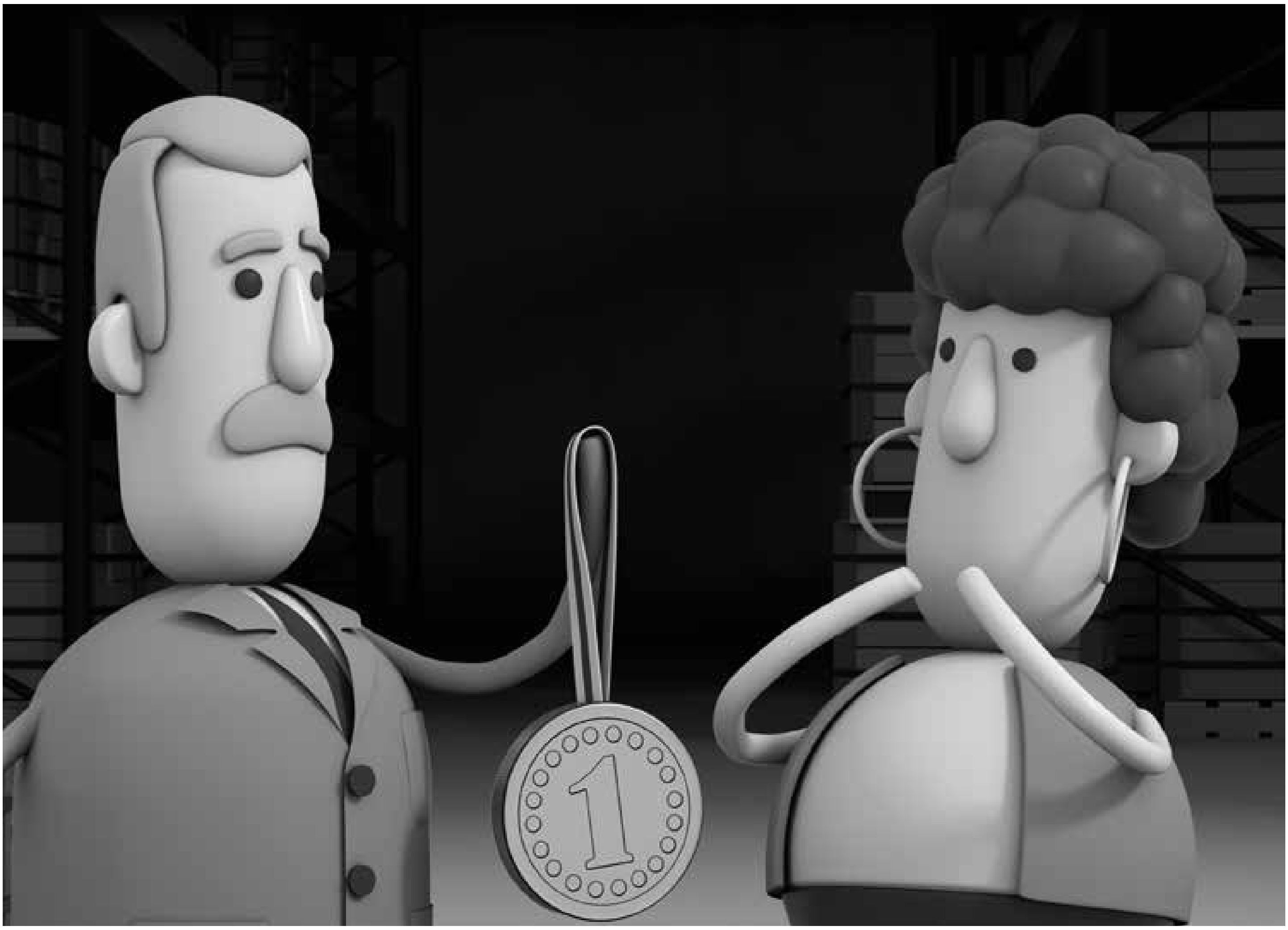
Running the 'It's OK to say' education programme



CPNI
Centre for the Protection
of National Infrastructure

Contents

Foreword

The ‘It’s OK to say’ programme is issued by the UK’s Centre for the Protection of National Infrastructure (CPNI) with the aim of helping organisations that make up the national infrastructure improve their protective security by raising awareness of the importance of speaking out in suspicious circumstances. It is general guidance only and is not intended to cover all scenarios or to be tailored to particular situations. It is not a substitute for seeking appropriately tailored advice in particular scenarios. You are responsible for implementing this programme within your own organisation in a way that complies with applicable laws and takes account of your particular business context. You remain responsible for your security including your protection from insider threats.

Acknowledgements

CPNI acknowledges and thanks the following for their work in the research and design on this programme:

- AML
- i to i research
- A Large Evil Corporation
- User Perspective

DISCLAIMER

To the fullest extent permitted by law, CPNI and each and every contributor to the “It’s OK to Say” Programme accept no liability whatsoever for any expense, liability, loss or proceedings incurred or arising as a result of any error or omission in the information or arising from any person acting, refraining from acting, relying upon or otherwise using the Programme.

Core Principles:

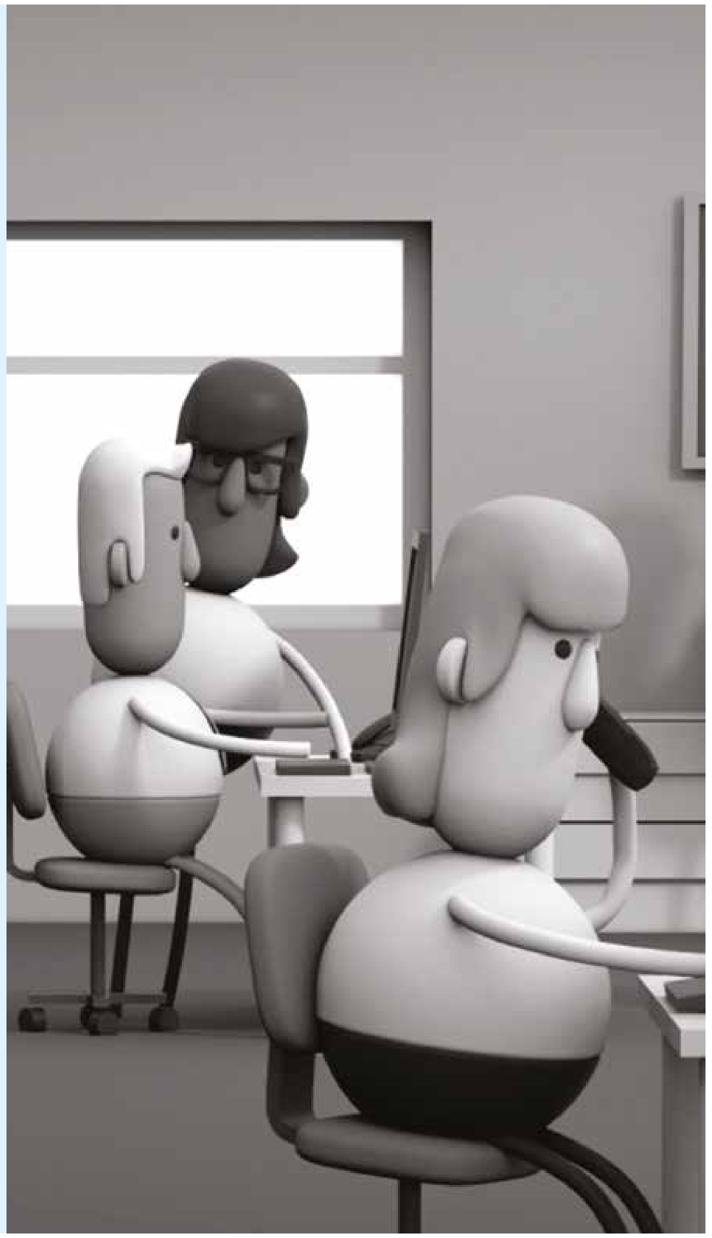
- Evaluate the benefit of adopting the programme in your organisation, then adapt it to fit your business context.
- Consider how to implement the programme ethically. Think about the potential negative effect on security culture if it’s not done in the recommended way.
- Establish and maintain policies and procedures on security, ethics, confidentiality and compliance together with your organisation’s legal obligations. Don’t forget data protection legislation.

Introduction

About this programme and the guidance

The ‘It’s OK to say’ programme has been designed by the Centre for the Protection of National Infrastructure (CPNI) to support organisations in educating their staff about unusual and unexpected workplace behaviour, and to encourage the reporting of that behaviour. This behaviour could be a sign of welfare or wellbeing issues or it could indicate something more concerning, such as a security threat or insider[1] activity.

The programme comprises this guidance, to be used to support an organisation in implementing an education programme, as well as materials and resources to support communications and training, all of which are referenced throughout this document. Designed to be modular, the programme provides the flexibility to trial, tailor and apply according to your organisation’s needs, culture and risk exposure.



A programme in two parts

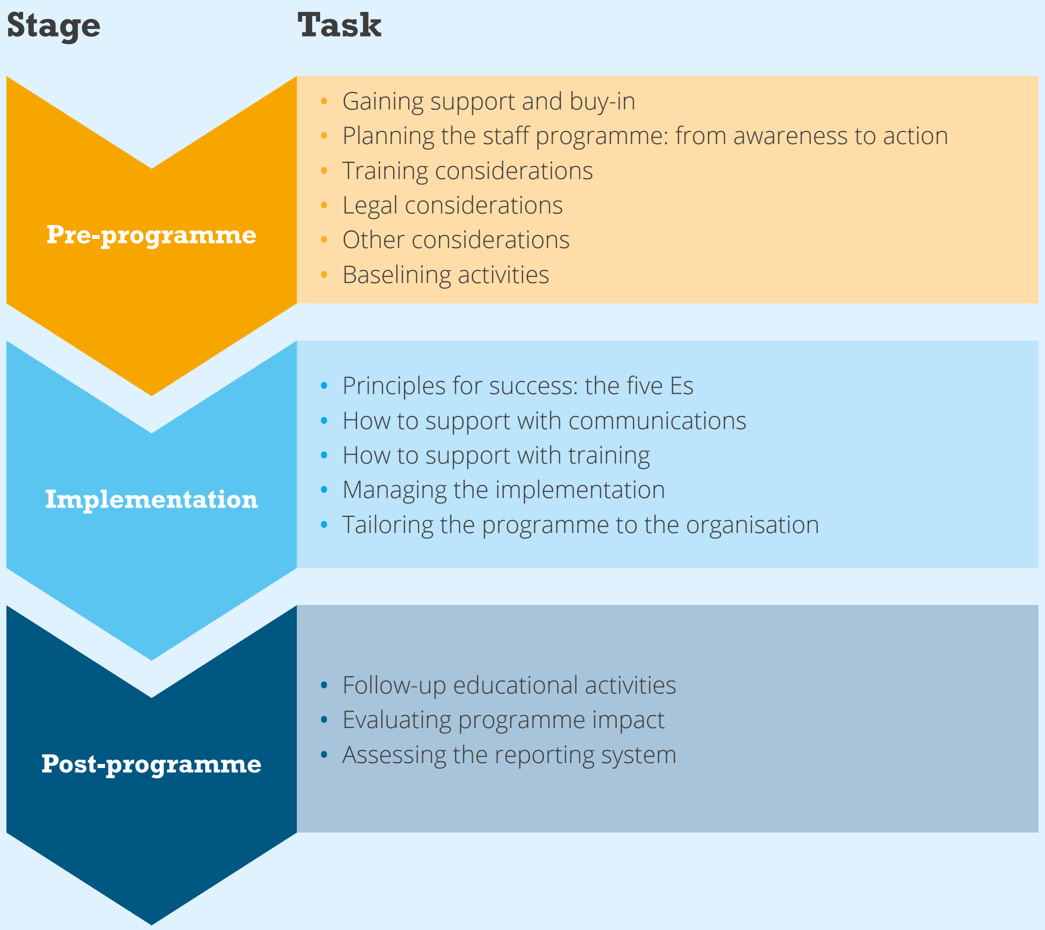
The recommended programme for staff education comprises communications and training. Both parts are flexible, enabling you to decide which elements will work best with your organisation and approach. The guidance provides additional resources to assist with programme design and considerations such as evaluating existing reporting mechanisms, programme implementation and assessment of the programme’s impact.

[1] For the purposes of this programme, an ‘**insider**’ is defined as: a person who exploits, or has the intention to exploit, their legitimate access to an organisation’s assets for unauthorised purposes.

How to run the programme

The diagram below suggests how a programme should be structured, outlining the key principles for success. Here we recommend three phases: pre-programme, implementation and post-programme, including where the communications materials and staff training fit best.

Programme Overview



Stage	Task
Pre-programme	• Gaining support and buy-in • Planning the staff programme: from awareness to action • Training considerations • Legal considerations • Other considerations • Baselining activities
Implementation	• Principles for success: the five Es • How to support with communications • How to support with training • Managing the implementation • Tailoring the programme to the organisation
Post-programme	• Follow-up educational activities • Evaluating programme impact • Assessing the reporting system

One of the key outcomes for this programme is to change reporting behaviour. There are five underpinning principles to organisational behaviour change, these are:

- **Educate** why
- **Enable** how
- Shape the **Environment**
- **Encourage** the action
- **Evaluate** the impact

These five principles are explored in a later section of the guidance (pages 17–19) and more detail can be found in the CPNI guidance ‘The 5Es to embedding security behaviours’.

The background to this work

This guidance builds upon research, undertaken by CPNI, within several organisations across different sectors in the national infrastructure. This research investigated what conditions would influence staff to intervene[2] in a proportionate way upon witnessing unusual and unexpected workplace behaviours. The approach and materials mentioned throughout have been developed with subject matter experts within these organisations and, in some cases, directly trialled on a substantial number of staff members.

The guidance emphasises a duty of care approach, encouraging staff to intervene out of concern for the individual but also for the knock-on effects he/she might have on the immediate team or the organisation as a whole. In short, it is designed to encourage your workforce to trust their instincts and take personal responsibility for staff welfare and security.

Unusual and unexpected workplace behaviour

Unusual and unexpected workplace behaviour (often referred to as 'behaviours' throughout this document) could take a variety of forms, sometimes emerging as a change in typical behaviour. These behaviours fall into one or more of these categories:

- Behaviours that suggest a potential individual vulnerability or risk (includes changes in work-related attitudes/ behaviour and signs of struggling with negative events, such as stress)
- Unexpected or difficult to explain work activities that cause concern (suspicious work activities)
- Work activities which are unauthorised, or may be authorised for some individuals but are not for others

Why an awareness programme should be considered

The implementation of a programme designed to raise awareness of unusual and unexpected workplace behaviour could involve considerable effort and other resources, and will therefore require some degree of justification. The following reasons are listed to help with this justification process:

To identify members of staff who may require support
Unusual and unexpected workplace behaviour can be indicative of a broad range of issues which could be financial, work-related or otherwise personal in nature. These particular issues, if left ignored, could cause the individual considerable distress but also raise their vulnerability to becoming involved in insider activity. If behaviours are identified in a timely manner, appropriate support can be put in place. This could potentially enable the individual to resolve their issues before more serious problems develop.

To protect the organisation and individual workers from adverse effects
The resolution of a staff member's issues is likely to have knock-on benefits for immediate colleagues and the team as a whole. Furthermore, a greater awareness of unusual and unexpected workplace behaviour may help to protect the organisation more broadly. An insider act could interfere with production, impair valuable assets and cause untold harm through reputational damage and loss of customer trust.

To enable the identification of a potential insider act
There is evidence that insiders tend to display a range of unusual and unexpected behaviour before committing an insider act. The identification of these behaviours could therefore help to prevent insider activity. Those who work closely with the insider are most likely to have the opportunity to identify behaviours although they typically go unreported by staff. This programme is therefore targeted at all staff members, to reduce the likelihood that unusual and unexpected workplace behaviour will go ignored by those best-placed to notice it.

Insider threat

Previous CPNI research[3] has shown that insider activity falls into five main categories:

1. **Unauthorised disclosure of sensitive information,** such as leaking information to the press for the purposes of reputational damage
2. **Process corruption**, essentially altering an internal process or system for an illegitimate aim, such as fraud
3. **Facilitation of third party access to an organisation's assets,** which could include premises, information or people
4. **Physical sabotage**, such as starting a fire in a key operational area
5. **Electronic or IT sabotage**, e.g. intentional damage to computer hardware

> Unless explicitly specified, we have used the term 'staff' in this document to mean permanent employees, contractors and/or third party suppliers. It is important to consider the target audience for the programme. Where do the risks lie? Who is best placed to spot these? Think about consistent messages and awareness levels across all relevant staff.

There are also three main types of insider, each defined by their intention:

- **The deliberate insider:** who seeks a job with the company, intending to exploit their access
- **The volunteer/self-initiated insider:** whose intent to abuse their access is a personal choice and develops during the course of their employment
- **The exploited/recruited insider:** who joined the organisation without any intent to misuse their access although is persuaded to do so by a third party, through exploitation or other means

Prevalence

CPNI's Insider Data Collection Study found that 76% of cases were self-initiated, 15% involved exploited/recruited insiders and only 6% resulted from deliberate infiltration.

Case studies and research into insider activity show that some of the most damaging acts are carried out by personnel in sensitive posts who are trusted by the organisation. It is the accesses afforded by their jobs that typically enable insiders to engage in these activities. CPNI's research found that 88% of the insider acts were carried out by permanent staff rather than contractors or agency staff. This emphasises the point that anyone within an organisation can be an insider. Insiders may be motivated by financial gain, retaliating against a perceived injustice or have a desire for recognition. Alternatively, they could be tricked into abusing their accesses or role-related knowledge by someone external to the organisation who has hostile intent.

This research also found that the duration of insider activity has a considerable range, in some cases extending over five years and longer (11%). This demonstrates that in the majority of cases, there are likely to be numerous opportunities to detect insider activity which are being missed. This is to the detriment of the organisation and its staff.

[2] '**Intervening**' in unusual and/or unexpected workplace behaviour covers many possibilities, for example: discussing concerns with a colleague or manager, 'keeping an eye' on the individual (monitoring) or challenging them (perhaps subtly). Intervening could also encompass making an official report to a manager, a confidential helpline, or to Security.

[3] CPNI Insider Data Collection Study: Report of Main Findings, April 2013. See CPNI website or your sector adviser for a copy.

Rationale for the programme

The programme has been named 'It's OK to say' as it seeks to not only inform people about unusual and unexpected workplace behaviours, but also to encourage them to act when they notice such behaviours. Identifying behaviours more efficiently is likely to benefit the organisation and its individual members for reasons already outlined.

CPNI research has found that noticing unusual or unexpected behaviour, and recognising that it represents some cause for concern, does not necessarily lead to staff reporting it (at least through official reporting channels). And this is where the training – in addition to the communications – comes in. Trials of the training component have revealed evidence that trainees:

- Would be more likely to intervene upon seeing unusual and unexpected workplace behaviours following training
- Are more knowledgeable of these behaviours and therefore more confident in recognising them
- Are more able to challenge the common belief that permanent employees pose less of a threat to the organisation than other types of staff (e.g. contractors)
- Are more aware of intervention methods

These learning objectives therefore form the rationale to running this programme:

Objective 1: Improve understanding of the insider threat

- Anyone can be an insider, in any context – from permanent staff to contractors; from lower-level staff to senior management
- Insider activity can have very negative consequences for individuals, teams and the organisation

Objective 2: Improve awareness of unusual and unexpected behaviours and their link to the insider threat

- These behaviours could suggest several things and many situations will be ambiguous
- Insider activity tends to be pre-empted by such behaviours, but not all these behaviours automatically signal an insider threat

Objective 3: Enhance knowledge of how people can report or intervene

- Respond in a way that seems appropriate given the circumstances and your preferences. Organisations should provide a clear set of mechanisms for staff to report behaviours of interest

Programme approach in a nutshell:

The philosophy underpinning this work is that it is beneficial to establish a work environment in which people take personal responsibility for contributing to security through their everyday activities and interactions in the workplace.

Pre-programme

Pre-programme

- Gaining support and buy-in
- Planning the staff programme: from awareness to action
- Training considerations
- Legal considerations
- Other considerations
- Baselining activities

This section will help you with the first stages of planning and developing the '**It's OK to say**' programme to enhance awareness of, and intervention in, unusual and unexpected workplace behaviour. Setting up the programme involves deciding on its aims and functions, as well as identifying what existing initiatives it will need to work with. For example, it will need to be ascertained whether the reporting system principles (as set out in this document) are consistent with your organisation's policies. The pre-programme stage will therefore involve a great deal of thinking and consultation over the core design of the programme, in order to make it fit for purpose within the organisational context.

Gaining support and buy-in

The programme will require a coordinated effort from all stakeholders, therefore having their support is key. To help with gaining their support and buy-in you should be prepared by considering the following:

- What are the overarching strategic objectives – why are you running the programme?
- What does success look like – what are you looking to see changed? Have you got the right benchmarks for evaluation in place?
- Do managers have the right attitude to support the programme? Do they have enough time to play a key role in it? Have they been appropriately trained to act if they do identify behaviours in their team, or if team members discuss or report behaviours to them?
- Are there any senior individuals within the business who are enthusiastic about security who can be 'champions' or 'programme ambassadors' for the 'It's OK to say' programme?
- Can you provide a rationale and justification for the programme if you are challenged by colleagues?
- Who needs to be involved to ensure the objectives are met? Who are the stakeholders, managers and leadership teams within security, business and communications? Have they 'bought-in' and have corporate issues been considered for each team? Have you considered all of the below listed groups? *Note that there may be others who should be involved depending upon the structure and nature of your organisation:*
  - **Corporate affairs and communications** – reputational issues, 'branding'
  - **HR & Training** – to extend education, include in staff induction and reinforce the reporting process
  - **Briefing of Security and Risk Officers** – to ensure they know how to respond to reports
  - **Service desk or helpline personnel** – to ensure they know how to respond to reports
  - **Security incident management** – e.g. Protective Monitoring who may be watching for unusual and unexpected behaviours themselves on the computer systems: Consider where they fit into the process
  - **Line management** – to prepare them for increased reports and how to respond
  - **Trade unions or staff representation groups** – to ensure aspects of employee rights are considered with regards to reporting
  - **Legal** – to ensure report information is treated appropriately, processes adhere to necessity and proportionality rules, and relevant legislation is understood

Planning the staff programme: awareness to action

Consider the staff journey – to help you plan the programme, consider the journey that your staff will need to go through to enhance their awareness of unusual and unexpected workplace behaviour and feel empowered to take action when they observe it. Firstly, they will need to notice these behaviours in the workplace: CPNI research shows that some level of awareness-raising of what unusual and unexpected workplace behaviour is and how it might appear to an onlooker will be necessary, especially if this is a relatively new concept for people. Also some members of staff may be better placed than others to notice when a colleague is behaving in an unusual and unexpected way: those who have been working in their current environments for some time and those who work in a close-knit team, for example. This may have connotations for targeting the programme. The programme will also need to raise awareness of the issues that these behaviours could indicate, and emphasise what the consequences of these may be on both the individual and/or the organisation.

CPNI has developed a suite of communications materials and a training package to help convey the messages of the programme. The programme can be tailored to suit your organisation but it is strongly recommended that it comprises both a communications and training element.

Remove barriers – the purpose of the programme will ultimately be to encourage people to intervene when they see unusual and unexpected behaviour. The best way of maximising this is to reduce barriers to intervening, by ensuring that people can intervene in the way that feels appropriate to the individual and ensuring that the reporting system upholds various principles, such as confidentiality. Enablers to intervening will also need to be enhanced, by ensuring that reporting is easy (e.g. by advertising reporting channels) and by creating a culture in which people feel that intervening in these behaviours is acceptable.

Review/design the reporting system – the first step is to identify the mechanisms for intervention/reporting. The programme components will need to reflect the organisation's expectations about how a member of staff should intervene if they observe a colleague behaving in an unusual and unexpected way. To do this, first define the reporting channel options by doing an audit. It may be useful to consult with colleagues and review actual security reports, compiling a list of where they originated from. Be wary, however, of the fact that the reporting of unusual and unexpected workplace behaviour is typically low in most organisations. So, security reports are unlikely to be the most accurate source of information. It is therefore beneficial to have a clear understanding of how your members of staff are likely to share these issues, which can be developed by carrying out a baselining activity (see section on baselining – Page 16).

Ensure the mechanisms are fit for purpose – our research revealed six criteria for deciding on a reporting system that will help reduce barriers to reporting unusual and unexpected behaviour at work.

Reporting system principles:

1. **Provide a range of options:** Align with staff preferences for dealing with the situation. Our research demonstrates that when someone has seen a colleague behaving in an unusual and unexpected way, they will typically want to gather more information before making an official report. In order to maximise the potential for staff intervention they should be encouraged to intervene in the way they feel is appropriate at the given time. Multiple options for intervening should be provided because people will want to respond in different ways, depending on the nuances of the situation – see Figure 1. Furthermore, their preferences may vary according to their role in the organisation. It is also a good idea to provide at least one or two different practical mechanisms for submitting reports – for example, a confidential hotline AND an email mailbox/intranet form/postbox.
2. **Make reporting straightforward:** The reporting mechanisms should not require staff members to decipher exactly what type of issue they have observed, for example determining whether it is a physical security issue or a matter for the corporate ethics group. If people need to diagnose the situation in this way they will be less likely to report it when the situation is more ambiguous.
3. **Enable a soundboard function:** Ideally the reporting system should enable a 'soundboard' function, via appropriate channels. This allows potential reporters to at least discuss their concerns with the helpline or their managers, even if they decide against making an official report.
4. **Uphold confidentiality:** The reporting process should uphold confidentiality as far as possible and be seen to do this reliably, in order to encourage people to make reports without fear of negative consequences. This is distinct from anonymity which, while it may improve reporting levels, is not necessary legally appropriate for many organisations. Typically, anonymity cannot be promised in cases that enter full criminal proceedings, as in these circumstances the reporter may be asked to give evidence. A legal specialist should be consulted to determine the process, and the organisation should publicise the process to staff at the outset in order to encourage confidence in the system.
5. **Provide thorough follow-up of reports:** The 'follow-up' process, which should be tailored for your organisation using the training materials (PowerPoint slides available from CPNI), is intended to provide assurance that reports will be followed-up fairly. It is important to reassure people that decisions will not typically be made on the basis of just one report of unusual or unexpected behaviour; other sources of available information will be used to create a fuller picture. The follow-up process is also likely to discourage people from making false reports about individuals for malicious purposes.
6. **Give feedback:** Ideally an individual who has made a report will receive some level of direct feedback. As a minimum, this would be a confirmation sent to the reporter which thanks him/her for this contribution and states there will be some investigation into the issue. This at least provides assurance that the issue is being processed and the report has not been ignored. Your organisation is also likely to benefit from providing some general information to all staff which highlights the successes of the programme, specifically by advertising the benefits of intervening by underlining any threats that previous reports have circumvented. The detail permissible in these forms of feedback will depend on whether:
   - The confidentiality of those involved can be maintained
   - Critical gaps in the security process will be revealed as a result

Providing a range of reporting options

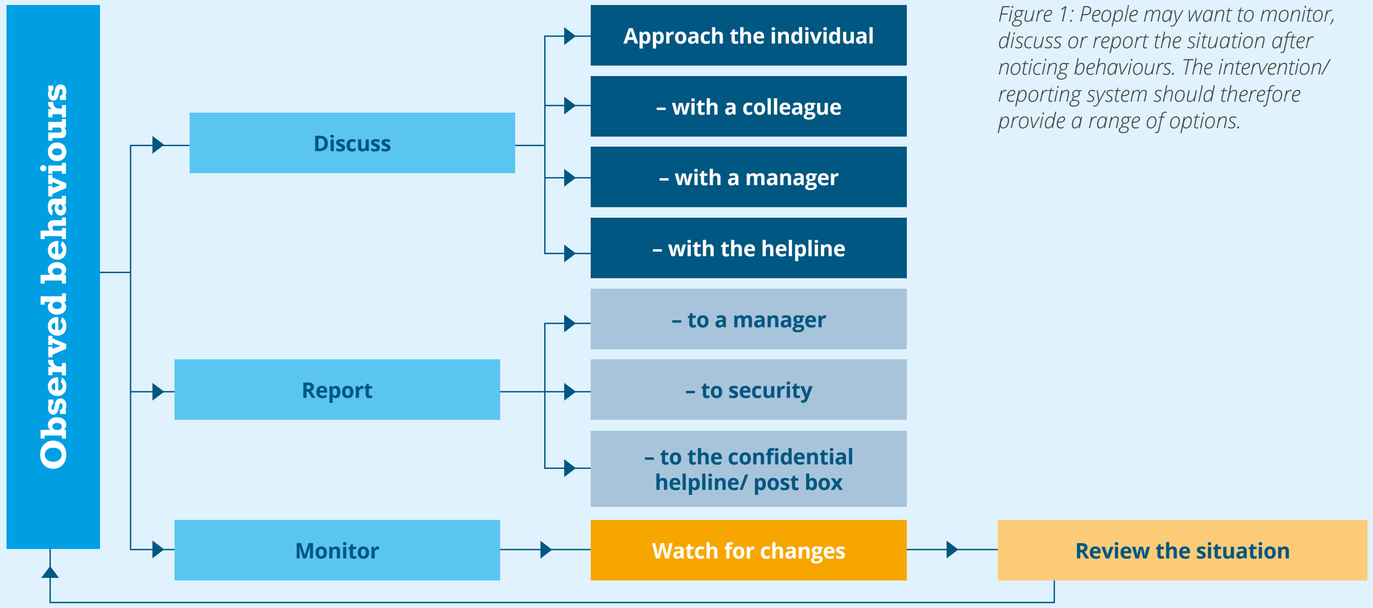


Figure 1: People may want to monitor, discuss or report the situation after noticing behaviours. The intervention/ reporting system should therefore provide a range of options.

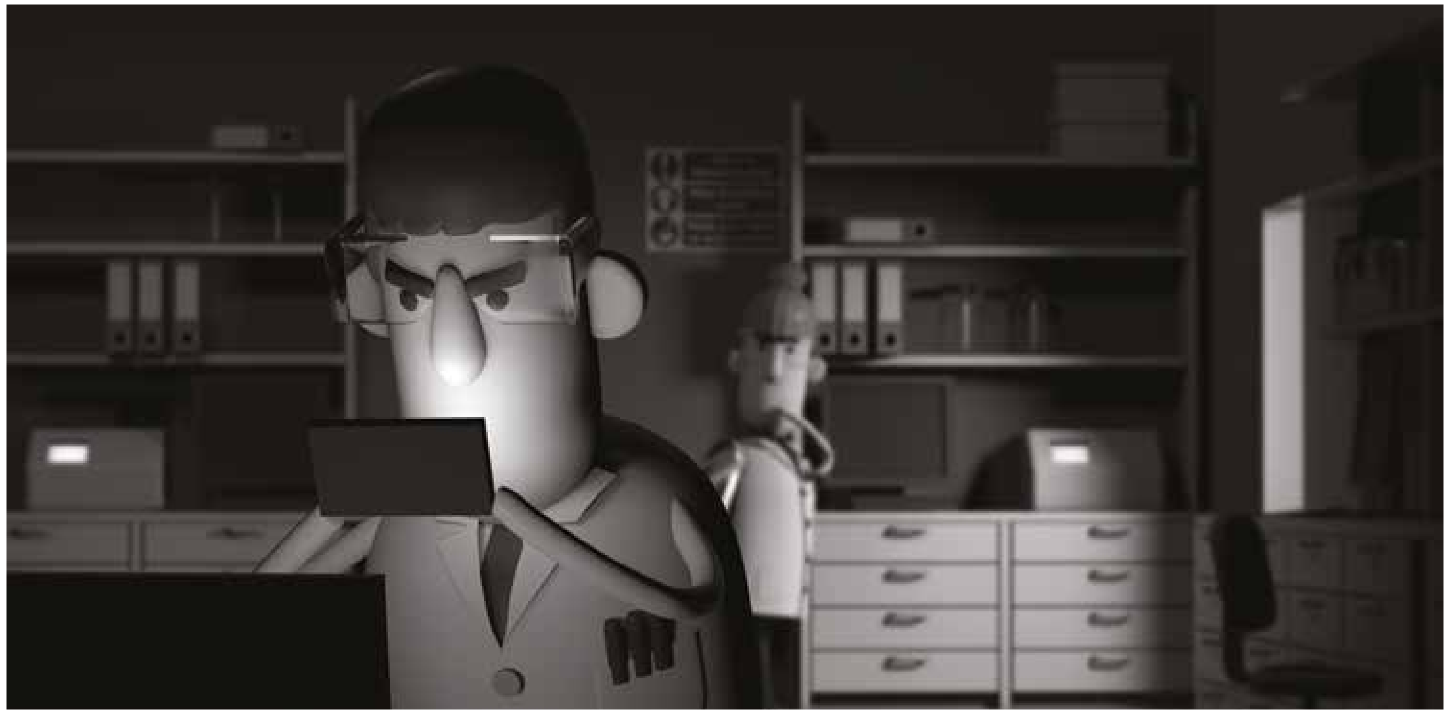
Handling, processing and communicating reports – once someone has made the decision to report it will be important that all of the reporting channels uphold the reporting system principles in the same way and information is gathered consistently. The following activities will be necessary to achieve this:

- **Plan training to support those who will receive reports**, e.g. line managers, helpline staff, etc. See sections on training (pages 21–25 for further details).
- **Design a form for recording reports** – the reporting process will need to be defined in detail and captured in a 'report form' (an example can be provided by CPNI on request). Consider whether the reporter's name will need to be requested at the point of reporting. While not requesting it will help to support confidentiality, anonymity may increase the opportunity for people to make false, malicious reports. It will also make it impossible to follow further leads and verify information with the reporter.
- **Feedback** – communicating feedback is an essential aspect of a reporting system loop, illustrating for actual and potential reporters alike, that reporting is a worthwhile endeavour and socially acceptable throughout the organisation. (See 'Potential pitfall 4' on page 18).

Scope of the reporting system – it is suggested that personnel throughout the organisation are given access to the reporting system, including contractors and permanent employees. However, there may be particular issues which prevent this from being possible for each reporting channel.

Reporting policies and procedures – some critical decisions need to be made about what will happen to the information that has been gathered. It is suggested that a thorough follow-up process should take place which draws upon other information to build a fuller picture. However, many questions will be raised in relation to this process, such as:

- **Who should be involved in any risk-based decisions?** Consider discussing reports at a working group, allowing for a considered approach to the risk any individual reported on may pose. Stakeholders from across the organisation can input their specialist expertise. The group should ensure confidentiality is maintained. If information relating to the report is written down, this should be on an appropriately secure and access-controlled system.
- **Information access** – who has access to this information and the peripheral information which is drawn upon?
- **Information storage and usage** – how long will this information be kept on file and what other purposes will it be used for? What is being formally recorded? If a hotline is used as a soundboard only, consider what should and shouldn't be written down or disclosed onwards. As an example of how confidence can be lost in the reporting process, if people suspect that it may be used to guide promotion and remuneration decisions then they will be reluctant to report, at least for the right reasons.
- **Decision making** – who will guide the overall process such as the decision about what outcomes should result from the follow-up? This may be the 'owner' of insider risk in the organisation, or a representative from a working group used to discuss reported concerns.
- **Approach to unofficial reports** – will any actions will be carried forward if someone chooses to discuss an issue but does not want to report it? It is recommended that this information is kept entirely 'off the record' so that people feel they have this intervention method open to them if the situation is too ambiguous for a more official approach.



Training considerations

Types of training: some staff will have a more central part to play in the programme. As such, training will differ to prepare them for particular roles. For example, those with line management responsibility could require coaching on specific skills and different objectives than are provided in the generic staff training that CPNI has produced for 'It's OK to say' (though CPNI advice can be provided on this if required). The training produced as part of this programme seeks to provide education that is suitable for all staff groups (including managers) about how, when and why they should intervene in unusual and unexpected workplace behaviour. It is equally possible to run this training separately or weave the content into an existing initiative (such as induction training or lunchtime talks). Refresher training should also be considered to remind trainees of key messages and to embed the importance of reporting behaviours into the fabric of organisational culture. An easy-to-read table of training options is featured in the Implementation section of this guidance.

How training will be disseminated: in large organisations, cascading training to site managers and training specialists may be the only feasible method of dissemination. This would enable managers to fine-tune training initiatives in line with the way people work on a local level. In smaller organisations, those responsible for training implementation are likely to have a greater understanding of job roles across all business areas. In these cases, a centralised approach to implementation may be more effective.

Who and when to train: while it is a good idea to train all employees/contractors (and potentially third-party supplier staff), this may be considered unfeasible or unnecessary. It is possible to train only those staff groups who have a particular need (e.g. those working in sensitive areas), relying solely on the communications and supporting materials to educate those remaining.

Managers – While training may be necessary to provide managers with sufficient knowledge and skills to deal with the effects of this programme, be wary of putting excessive responsibility on them.

New staff – Consider whether new inductees will benefit from the full training or if a reduced version is sufficient to get the main messages across. There is a balance to be struck here. These new employees and contractors represent an opportunity to make a substantial impact on your security culture. At this stage in their tenure, staff will be particularly open to new ideas and ways of doing things. The animation could also make a great introduction to security in general. While it addresses serious issues, it could be used to provide light-hearted entertainment to complement the delivery of other induction messages. Conversely, staff will need some knowledge of their working environments in order to identify unusual and unexpected behaviour. So it may be appropriate to delay this training until staff have 3-6 months of experience in the role.

In terms of when to train, consider how the training is best combined with the communications. Three options are available:

a) **After the communications** – This is the recommended sequence because the communications act as a 'warm-up' to the training, softening attitudes towards the programme that could thwart its success.

b) **During the communications** – The training and communications complement each other so it is possible to disseminate them together. This approach may be less effective in the long run because learning tends to be enhanced when initiatives are spread out rather than clustered together in time.

c) **Before the communications** – When training comes first, the main purpose of the communications will be to remind trainees of key messages. While the communications would be an effective reminder, trainers will probably meet more resistance to the programme concepts during training sessions if these have not been introduced before.

Trainer preparation: trainers will need to understand their specific role in the programme. The level of training required is likely to vary; those with line management responsibility, for example, may need coaching on specific skills.

Trainers should also be supported with advice on how to deal with queries and concerns from trainees that may be experiencing some level of resistance to the programme concepts. This will help equip the trainers to respond to challenging questions. Some typical questions or comments in resistance to the programme messages might be:

Comment: It is not my role to identify security issues.

Response: To tackle modern security threats we are all being asked to take greater responsibility for security – at work and in our personal lives. Our vigilance is expected in public places (e.g. public transport) just as it should be in your workplace.

Comment: I would know if my colleagues were up to no good.

Response: We acknowledge this. You could be in the best position to recognise a colleague who is behaving in ways that are unusual or unexpected. Typically, colleagues of an insider notice their unusual behaviour prior to the act, but shrug it off rather than take action. This has historically had serious consequences.

Comment: We don't 'spy' on each other here.

Response: You're not being asked to 'spy' on your colleagues or even become hyper-vigilant. This is about providing you with a way to share concerns rather than ignore them. In addition, insiders may be manipulated – it may be that your colleague is unaware of how their behaviour can impact on the organisation and they would welcome your intervention.

Comment: We trust each other implicitly.

Response: Anyone, including you and I, could be vulnerable to manipulation. Insiders also tend to be in trusted positions (where they have access to sensitive information).

Comment: This programme could undermine the trust I have in my colleagues.

Response: Unusual or unexpected workplace behaviour could be a clue that a colleague needs support; insider activity is just one possibility amongst many. Equally, you need to trust your colleagues. This programme is not asking you to question their every move, it is allowing you to share concerns that may or may not develop while you are at work.

Legal considerations

At the outset of implementing this programme, an organisation's legal department must be consulted. When setting up a reporting system, organisations may need to consider rules and questions in regards to relevant legislation (see overleaf). Note that this list is designed to highlight potential issues and encourage engagement with legal specialists – it is not exhaustive and CPNI accepts no liability for its content.

CPNI recommends that each organisation ensures a policy is written and communicated in language that is understandable to staff about the processes involved in any reporting mechanism. Additionally, organisational processes that relate to such legislation should be documented to ensure the decision-making process is understood should it be questioned at a future date. This is to help ensure consistency, fairness and thoroughness of the process.

Example Questions and Considerations

Necessity and proportionality (Human Rights/Data Protection)	• What are you recording about an individual (both the individual reported on, and the individual reporting)? Are you recording only what you require to mitigate the risk? Consider how intrusive you really need to be (Human Rights Act 1998) • Why are you recording it? Ensure you are not breaching any discrimination legislation • Are you happy to disclose the recorded information should it be requested by the individual(s) involved? (Freedom of Information Act 2000, Data Protection Act 1998)
Data Protection	• Is any personal data you are collecting stored securely? Is access to it audited? And are the access logs actively checked to assess misuse? • Is any of the information collected classified as 'sensitive personal data' under the Data Protection Act? Have you put in place the required measures to protect this sensitive data? • Does the method of storage (and access) meet the legal requirements of the jurisdiction the data is stored in? • If anonymity and/or confidentiality is to be upheld, the organisation should make assurances of this: will the processes withstand scrutiny both internally and through litigation? Does the way the data is stored and/or shared uphold confidentiality? Are there good reasons for anonymity (if used)? • How long are you retaining the data for? What is the justification for that retention period? • Are there any relevant exemptions from Data Protection law? These should be considered and applied on a case-by-case basis – for example, for national security reasons
Employment Law considerations	• Ensure any policy for employees outlines the limits to anonymity (where relevant) – for example, the organisation is likely to make its own judgement on maintaining the anonymity of any reporter once the organisation has become aware of a potential threat to the organisation or an individual • Consider the duty of the organisation to respond to all reports and ensure policies are in place regarding malicious reporting
Public Interests Disclosure Act 1998 (as amended)	• There may be other considerations when setting up a 'whistleblowing' mechanism. This legislation protects whistleblowers (reporters of wrongdoing) from detrimental treatment by their employer
Of public sector relevance	• Organisations should be aware that there may be additional duties and liabilities including those associated with malfeasance in public office and public interest immunity

Other considerations

- **Putting evaluation in place:** prior to rolling out the programme you will need to consider how it will be evaluated. This will be important in gaining ongoing support for the programme and similar initiatives. There is considerable guidance in the 'Post-programme' section and the template materials should only require small adjustments to work for your organisation. These materials need to be ready for implementation post roll-out, although if you are hoping to benchmark progress they need to be finalised before roll-out.
- **Adapt aspects of the programme in light of recent events if necessary:** recent events which have caused bad feeling and distrust amongst personnel could leave a residual degree of cynicism. In such circumstances various claims of the reporting system, such as the promise of confidentiality and how the information will be used for the purposes of the 'Follow-up' process, may not be believed. It is unlikely that the reporting system will be trusted if this is the case. In contrast, where there is a high level of trust amongst staff, it may be less important to emphasise these kinds of assurances.
- **Timing:** think carefully about the launch of 'It's OK to say'; consider whether the planned launch date will clash with any other communication and training initiatives or come at a particularly busy period for programme participants.

Baselining activities

Pre-programme baselines – some organisations may be interested in learning how their staff currently view unusual and unexpected workplace behaviour, their likelihood of intervening and their preferences for responding or reporting. They will want to conduct baselining prior to introducing or refining reporting mechanisms to help understand the effectiveness of their existing channels.

Putting measurement – and metrics – in place from the outset will be of benefit when it comes to refining the programme further down the line.

Other benefits

- Providing a 'baseline' from which the impact of the programme can be measured
- Evaluating existing reporting channels and determining how they can be improved
- Understanding whether people have particular barriers and enablers to reporting (or intervening) which could be targeted directly with the design of the programme
- Establishing support for the programme before it is launched by highlighting any limitations with existing mechanisms or insider threat awareness
- Understanding what people's preferences are with regard to intervening in behaviours, to aid the design of the staff intervention/reporting system
- Gaining further understanding of the existing initiatives within the organisation which are considered to be related
- Producing a wealth of information about the particular behaviours that are considered more common/concerning in different working environments, so as to enable training scenarios to be tailored to the organisation and its business areas

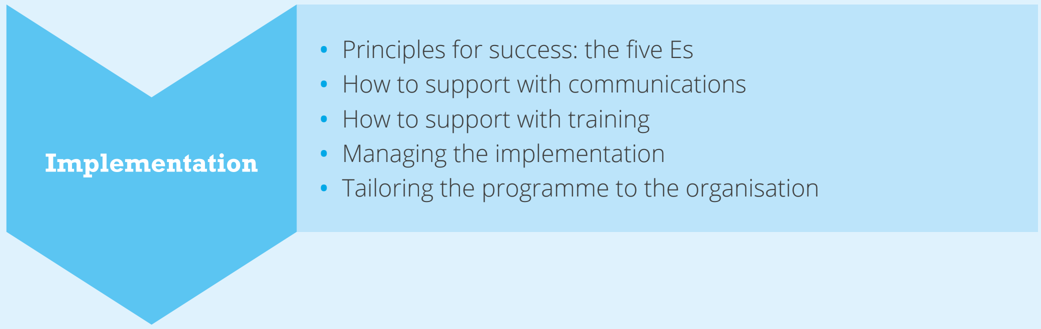
Methods for baselining – there are a vast array of methods that could be used to carry out baseline research on your organisation. As part of our research, we have trialled several methods and have refined a flexible, interactive one which enables a range of complementary information to be collected. We refer to this as 'baseline workshops'. These are especially appropriate for running with groups of staff who are of a similar grade to one another, although they can be drawn from across different areas of the business if desired. They involve two components:

1. **Group discussion questions** – encouraging attendees to share their opinions about issues of relevance to the programme. A question set for this purpose is available which can be edited to better fit your organisation's features and priorities, or used as it is (see Annex of Resources).
2. **Self-report questionnaire** – allowing attendees an opportunity to express their specific perceptions of (and expected reaction to) a hypothetical scenario depicting concerning and unusual behaviour. This method can easily include additional questions intended to gauge aspects of security culture. This provides a more stringent way of understanding and comparing your target programme audience.

Running a set of baseline workshops can involve many groups of staff members, or just a few. The number of baseline workshops you hold will be governed by your resources. While it is true that running just one or two workshops will be better than nothing, holding more workshops than this will make the resulting information more robust and dependable. There are several things you will need to think about if you plan to run a research activity such as this; see (See section on 'Evaluating programme impact' on page 27 onwards). For assistance with gathering, interpreting and presenting the findings from the baseline workshops, please contact CPNI.

Another simple method of obtaining a baseline of staff's current perceptions of the risk and the reporting mechanisms could be to put out a short survey to staff. This could be held on the organisation's intranet, allowing as broad a range of staff as possible to submit their views and to gauge their level of awareness. Please contact CPNI if you would like help creating such a survey.

Implementation



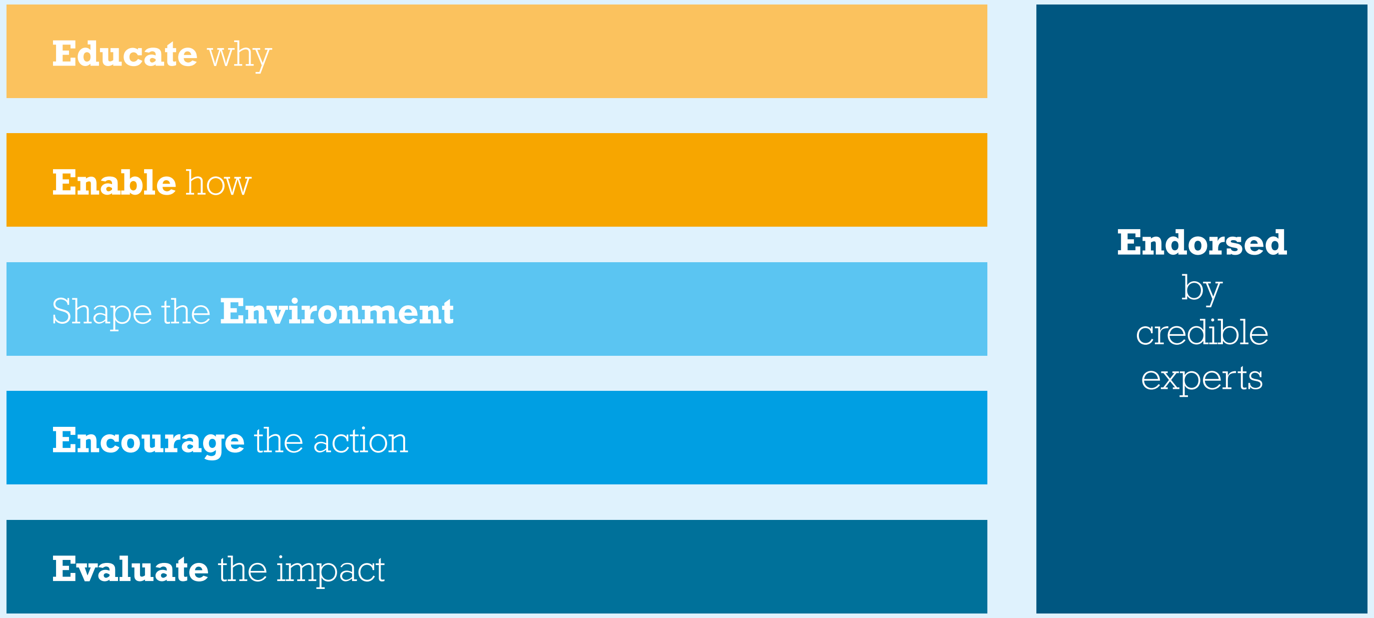
- Principles for success: the five Es
- How to support with communications
- How to support with training
- Managing the implementation
- Tailoring the programme to the organisation

This section discusses the '**It's OK to say**' education programme implementation in detail. It consists of a communications and a training part, both of which are made up of modular components which can be selected as appropriate and adjusted to fit the needs of your particular organisation.

Principles for success: the five Es

There are five underpinning principles which should serve as a checklist of what needs to be in place to deliver organisational behaviour change and have a lasting impact. They are key to the success of this programme, see diagram below:

The 5 Es to organisational behaviour change



Educate why

Enable how

Shape the **Environment**

Encourage the action

Evaluate the impact

Endorsed by credible experts

Each of these is briefly explained with examples of where the programme could face challenges if the principles were either not applied, or badly applied.

Educate why – Education is crucial to encourage staff reporting. Unless staff understand the insider threat – that it can happen and have serious consequences to both staff and the organisation – unusual or unexpected workplace behaviours continue to go unchecked.

Potential pitfall 1 – The animation is used on its own	
Example issue:	The animation is placed on organisation's intranet without any supporting communications or context provided.
Effect:	Staff consider the animation to be simply an amusing security video. There is no communication to staff on the serious message that it relates to insider threats in their organisation, and that behaviours of concern should be reported. Staff remain unaware that insider threats are a very real risk.

Enable how – Explain the vital part staff can play in mitigating the insider threat by their actions and behaviour. The organisation should communicate what unusual and suspicious behaviour looks like, and develop the right skills to enable staff to identify and report these.

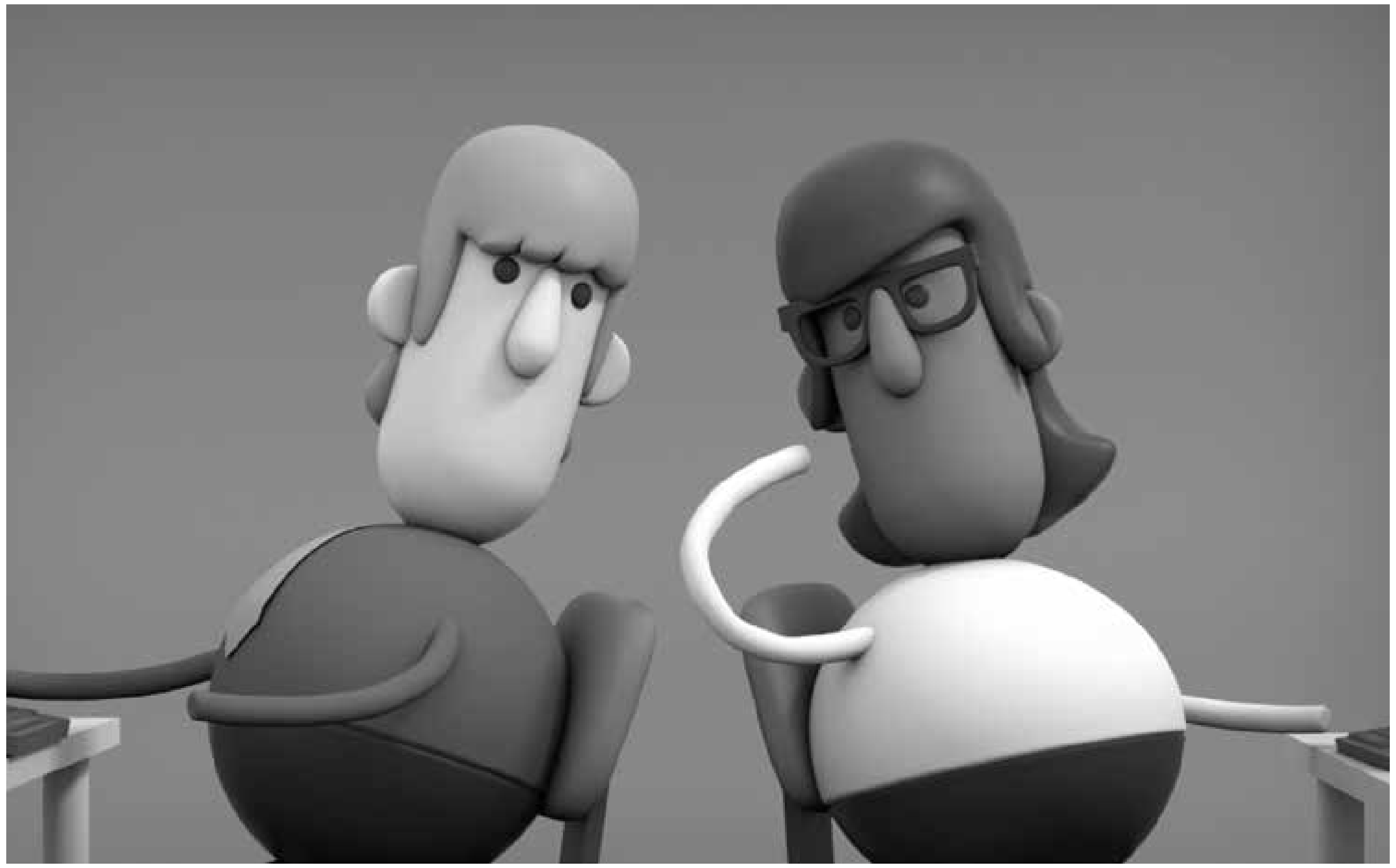
Potential pitfall 2 – Staff are not provided with adequate training on behaviours of concern	
Example issue:	Staff are aware of the insider threat, but are told only that they should report 'suspicious behaviours'. No training session to allow for open discussion of what these behaviours may be has been provided by the organisation and staff are ill-equipped to understand what they should and shouldn't be worried about.
Effect:	Staff report either too much or too little. There may be numerous false positive reports, which those responsible for handling them may not have the resources to deal with. Both parties lose confidence in the programme, and a sense of mistrust may prevail amongst staff in the organisation as trivial issues are reported, or serious issues are not dealt with.

Shape the **Environment** – Create a physical environment that makes staff intervention and reporting easy. Establish the social environment by making any good security behaviour the 'norm'. Give people permission to trust their instincts and intervene where they feel something is not quite right.

Potential pitfall 3 – Lack of appropriate reporting mechanism	
Example issue:	Staff are given a long list of reporting hotlines to contact for different and varying behaviour types; some or all lines are not set up in time.
Effect:	Staff are left confused as to whom to report behaviours that are not listed; confidence in the process is quickly lost when they cannot speak to someone. Future behaviours go unreported. No warning of possible insider act or welfare concern.

Encourage the action – Behaviour change can only occur if the organisation is seen to reward good behaviour. This does not mean necessarily in material terms. It is about recognising and reinforcing the behaviour and culture you want to encourage. Equally, the converse applies; where staff have failed to act when they've seen something wrong there need to be measures in place to follow up as to why this happened. You may like to publicise internally examples of real-life insider threat scenarios where reporting concerns produced a positive outcome (for all involved), and those where a failure may have led to a negative outcome.

Potential pitfall 4 – No feedback process	
Example issue:	A member of staff notices that a colleague is acting strangely and differently and reports it to the reporting email mailbox. They receive an automated response stating that their request will be looked at within 24 hours. They subsequently hear nothing.
Effect:	Individual who reported concern has no idea whether they have done the right thing. They may see the behaviour they reported continue, and be confused as to how to further progress the issue. They lose confidence in the reporting process and are unlikely to do it again should they see such behaviour elsewhere. Alternatively, they may intervene more directly themselves when in fact a follow-up has already begun, which may cause serious repercussions for the investigative process.



Evaluation – When running a programme it is important to know if it is working to effect behaviour change. This way, you can improve any shortcomings and build on successes. Processes should be put in place to enable a consistent, fair and thorough investigative process which will allow for good metrics as to the effectiveness of the programme. The programme should be evaluated to help measure this by comparing a baseline before and after the programme is implemented.

Potential pitfall 5 – Reports are not captured consistently	
Example issue:	Reports come into a central hotline and a working group discusses the concerns, but do not have a set policy for dealing with them. If challenged, working group members are not able to justify their decision-making or confirm metrics that may allow a measurement of success for the programme.
Effect:	Programme impact unknown; stakeholders may become unconvinced about programme efficacy; support for the initiative is withdrawn; and a potentially negative impact on reporting behaviours could begin to manifest.

Underpinning the Es is Endorsement – This is about ensuring the support of key stakeholders and credible experts in the organisation, ensuring that they are aware of, and back, the programme. Such endorsement is critical for the success of the programme; unless management have a positive attitude to the programme – and are prepared to find time to play a role in it – the good education effort will be wasted. Equally, you should consider who is best placed to deliver the required key messages. Credible experts, in tandem with management, that are seen to be enacting the types of behaviour change they are endorsing will be crucial. As one example, it may be that some areas respond better to the 'It's OK to say' programme when it has a welfare rather than a security-focused message.

How to support with communications

CPNI has developed a suite of communication materials to support you. They will help to educate staff on the behaviours that we are asking for them to spot and help stop. What you use is up to you.

The materials draw on the central theme of 'It's OK to say' and help give staff 'permission' to intervene and report, whilst providing the options for them to speak out. The ideal programme design is to warm up using the short animation and follow up using the other supporting materials.

Animation – this short film explains how behaviours are manifested in an entertaining and engaging way, introducing the 'It's OK to say' message and covering many examples of the behaviours that may be indicative of an insider threat. It's easy to share with staff and makes for a strong starting point. The original animation is available from CPNI, but we have included a storyboarded version for reference – see Annex (pages 36–37).

Posters x eight themes – these posters are designed to act as a reminder of the key communications messages and maintain a 'buzz' around the training. The poster themes pick up on the main scenes from the animation. Customisable, they allow you to include your organisation's logo and specific action options; whether this is approaching the individual acting unusually, having an informal chat with a colleague or reporting their behaviour.

A range of posters has been provided to enable you to 'refresh' the messaging periodically (we would suggest after 6-12 months). The range also gives flexibility to choose posters that best meet organisational goals. See the Annex for minimised versions of the individual posters.

Reminder cards x two versions – working in conjunction with the posters, these can be handed out or desk-dropped to staff following training. Again, these allow you to add your own process for intervention and reporting of behaviours.

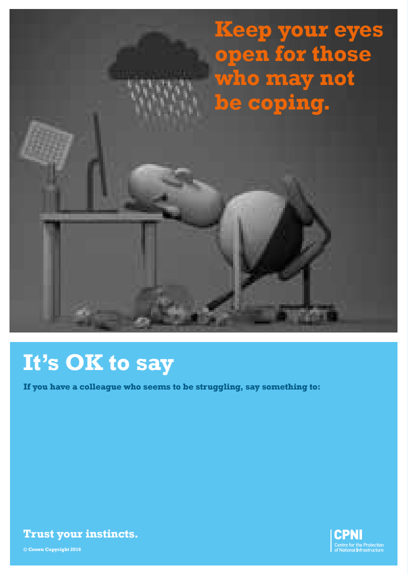
The communication materials are designed to provide both the 'warm-up' and 'follow-up' to tailored staff training. However, they can also be used as stand-alone educational tools.

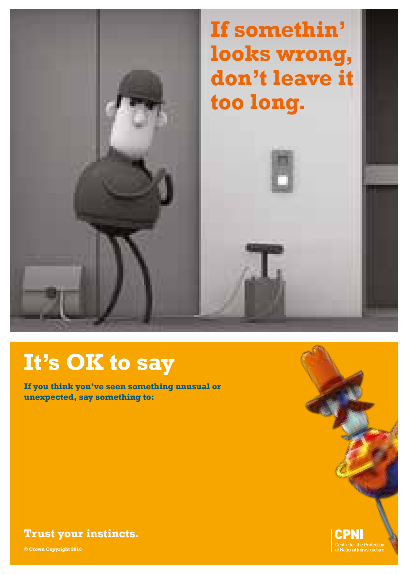
Digital communications – characters from the animation can be used in your digital communications such as your intranet site to reinforce and amplify the key education messages. In addition, the characters can be dropped into emails from those that have received training to remind people of the more detailed training content. These assets are provided as part of a suite of communications materials.

Examples of the supporting communications materials are provided in the Annex and full resolution versions are available from CPNI on DVD.

To request these editable artwork files and/or access to the animation please email CPNI at: **enquiries@cpni.gsi.gov.uk**

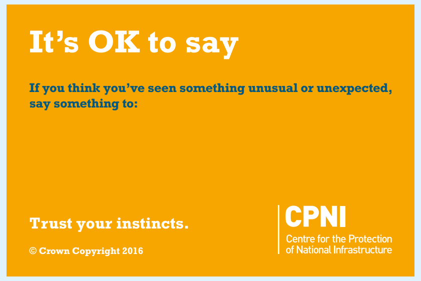
Posters


Keep your eyes open for those who may not be coping.
It's OK to say
If you have a colleague who seems to be struggling, say something to:
Trust your instincts.
CPNI


If somethin' looks wrong, don't leave it too long.
It's OK to say
If you think you've seen something unusual or unexpected, say something to:
Trust your instincts.
CPNI

See Annex of Resources for the full set of materials available.

Reminder Cards



It's OK to say

If you think you've seen something unusual or unexpected, say something to:

Trust your instincts.

© Crown Copyright 2016

CPNI Centre for the Protection of National Infrastructure

Phasing the programme

The ideal would be to roll out all the communications and training components as set out in the diagram below – but you may want to adopt just selected elements. For example, choosing not to use the animation, or to use the communications materials alongside your own existing training around insider threat or staff welfare issues.

The communications materials have been designed to support three distinct phases:

1. **Warm-up**, using the animation.
2. **Follow-up**, where reminder cards are disseminated to those attending training, and an initial selection of posters are sited in appropriate areas (see section below on siting).
3. **Refresh**, where the remaining posters can be used to keep the messages fresh. Again, this should ideally sit alongside training (e.g. refresher training).

See Figure 2 below.

Siting the materials – think about restricted areas; the posters may be particularly appropriate for sensitive or high-risk areas. There are specific posters that feature restricted areas like control rooms. Consideration should also be given to where you can reach the maximum number of staff (such as exit and entry points), whether they would work better in discreet locations (to trigger a phone call there and then), and dwell time (see below).

Dwell time – think also about dwell time for the posters. This refers to how quickly people move through any given area. At areas with high dwell time, like a staff notice board or canteen, people will be hanging around and will have time to read. At areas with low dwell time, like the main entrance to a building, people will be less inclined to read anything in detail.

Conflicting with other campaigns – ensure the posters do not conflict or confuse staff by sitting next to other campaigns (for example, if you were establishing a new reporting mechanism that was not outlined on this poster set). Staff are also less likely to notice a specific campaign poster if it is run in conjunction with several other messages at the same time. Try not to bombard staff with information all at once.

How to support with training

Embedding education on how to spot unusual and unexpected behaviours in the workplace is best achieved through training. Training can be implemented with or without use of communications, however, the ideal programme design should include internal communications and training.

CPNI trials show that the training package makes staff more aware of these behaviours and more knowledgeable about how to intervene. Following training, staff understand the importance of taking action upon seeing colleagues behave in an unusual or unexpected way and express a greater intention to intervene. As with any education programme, refresher training is recommended to embed the messages and desired behavioural change.

In addition to staff training, there will be a need to prepare managers because:

1. They are typically in a good position to identify unusual and unexpected workplace behaviour (assuming regular contact with team members).
2. They need to feel that identifying these behaviours amongst the team is within their role remit.
3. Our research also shows that most staff would prefer to discuss an issue with their line manager when first noticing these behaviours. As the most popular channel for official and unofficial reports, it is crucial for line managers to uphold the principles of the reporting system (such as confidentiality and providing feedback).

> Managers will need support and encouragement to endorse the programme. Their responsibilities should be outlined clearly, as well as the support and escalation options available to them.

The ideal roll-out

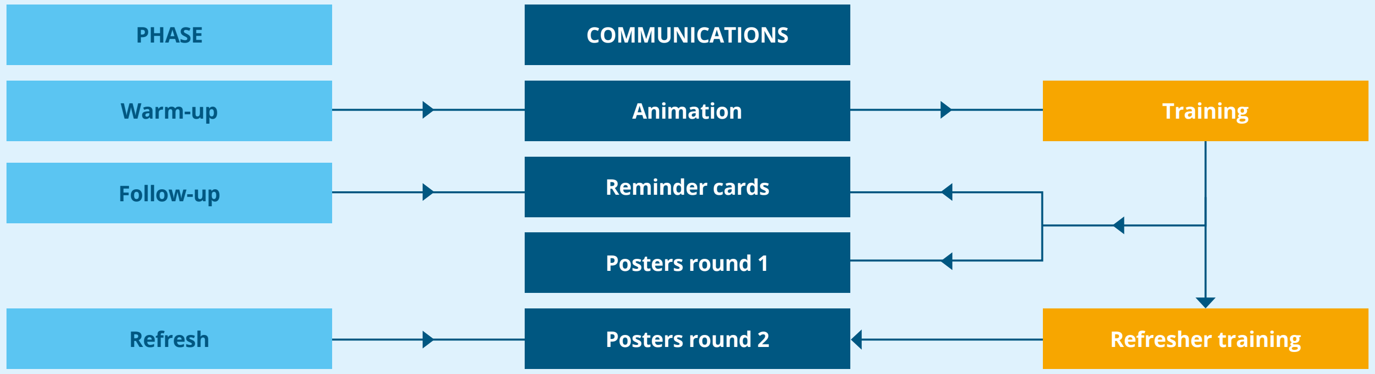


Figure 2 – How to phase the communications.

In the table below a checklist has been provided which sets out the recommended training aims, methods, content and duration as well as detailing the CPNI materials available to support organisations in training different groups of staff.

Checklist for Training – By Intended Audience

	TARGET GROUP		
	STAFF To consider: Permanent employees; contractors; suppliers; temporary staff; sensitive positions or areas.		MANAGERS
	INITIAL TRAINING	REFRESHER TRAINING	
Aims & learning objectives	Educate on insider threat* (and other relevant vulnerabilities) Education on link between insider threat and unusual and unexpected workplace behaviours Encourage to take action Inform on reporting channels/ intervention options Make clear how the reports will be dealt with. Instil confidence in the process Ensure staff know concerns will be dealt with effectively and confidentially **Note – some organisations may want to soften the focus on security and put the emphasis on staff wellbeing instead*	Reiterate the key messages of the initial training	Prepare managers who are likely to receive reports and brief them on the whole programme and specifically: • Relay the key messages of the 'It's OK to say' programme • Describe how both official and unofficial reports should be received and how the information should be treated (e.g. confidential) • Emphasise the importance of trust and feedback in encouraging reports from team members • Detail how the reporter should be provided with feedback (level of information, timeliness, confidentiality, etc.) • Explain what other information may be available to managers • Describe whether and how they should log the information gathered to support an audit trail of their decision-making • Help them to think through how unusual or unexpected workplace behaviour might be explained, given the individual and the context • Provide an understanding of where managers can receive support • Instil an appreciation of the appropriate actions in given circumstances, providing specific contact details for making referrals
Methods	Trainer-led and interactive	Mixed Interactive and/or remote	Written and/or verbal format from Senior Management
Content & subject areas[4]	1. Learning objectives 2. Scenarios depicting behaviours – consider using scenarios from historical insider cases in your organisation 3. Options for reporting and intervention	Summary of initial training Share programme evaluation findings Share success stories resulting from staff interventions Use case studies from other contexts Expert talks	Cover key steps in the reporting cycle: - Their role in raising awareness among staff of unusual and unexpected workplace behaviours - Guidance on receiving information – assurance of confidentiality and actioning of report - Where to go to seek further information having received a report - Advice on how to decide – and act – on the right course of action - Providing feedback to the reporter. Briefing on the 'It's OK to say' programme
Duration	45 minutes – 1 hour	No recommended duration	No recommended duration
Materials available	Scripted PowerPoint slides Segments of group discussion Audio scenarios depicting examples of unusual and unexpected behaviours	Case studies Shortened versions of the materials for the initial training with new scenarios Consider an outside speaker to give a talk on insider threat or staff welfare issues	Other CPNI guidance – for example, 'Ongoing personnel security' and 'Line Manager's Campaign' Campaign materials Template – 'It's OK to say' briefing note
Adaptation required for your organisation	Learning objectives Handling reports and reporting mechanisms/preferences Scenarios – to be realistic and relevant ('it can happen here, and it could happen to this section of the organisation, for this reason' etc.) Length of training Look and feel of PowerPoint slides – amendment to escalation slides to incorporate organisation's reporting mechanisms Outcomes – emphasis in terms of insider threat versus staff welfare issue	Success stories from your organisation Evaluation findings	Format for delivery of the training Template – 'It's OK to say' briefing note

In summary, the key aims of the training will be to educate staff about what the threat is, how and when they should intervene in unusual and unexpected workplace behaviour (what this is), and why they should take the trouble to do so.

[4] Content is available to support each section, see PowerPoint slides referenced in 'materials available' above and in the resources Annex to this document and available on the CPNI extranet.

Integrating the training – the training should ideally be complemented by the communications, which provide both a warm-up and reminder of the key messages. Various training options are available depending on what you feel would be most appropriate and effective for the target staff members and their working context. The animation and follow-up communications emphasise learning around '**what**' should be acted on (i.e. behaviours) and '**how**' to intervene (i.e. the intervention/reporting options). The training emphasises the '**why**' and '**when**' aspects more directly but goes a little deeper into what by exploring the behaviours/activities in a more context-relevant way. The '**why**' message involves promoting the fact that acting upon behaviours will help to prevent various harmful outcomes for the individual, the team and/or the organisation. The '**when**' message is concerned with immediacy and trusting gut instinct rather than waiting for absolute certainty. The key messages relayed in the training relating to when and why people should intervene can be repeated in long communications such as articles and intranet postings to ensure they are not forgotten.

Running the training

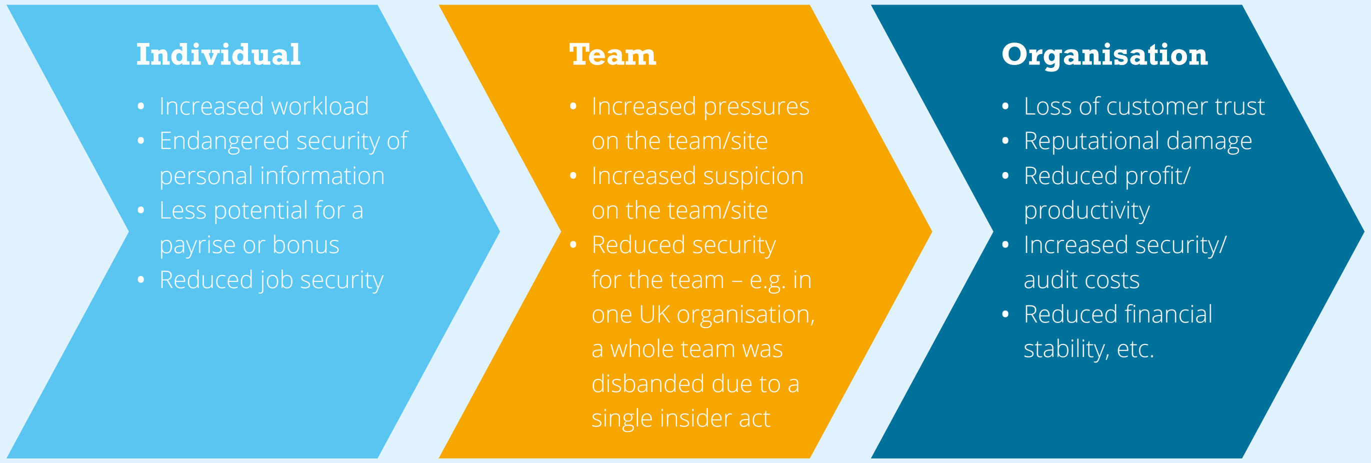
Key tips – Ensure staff training involves some degree of interactivity. By enabling trainees to discuss the training messages with one another and the trainer, the material can be absorbed more fully and contrary attitudes resolved.

Representing the behaviours: Be wary of lists

- A list of example unusual and unexpected workplace behaviours can be helpful in illustrating how they could look. However, it would be risky to provide training on exactly 'what behaviours to look for' in a checklist format. This is because if a member of staff sees a behaviour not on the list, but that they are uncomfortable with, they may be confused as to whether to report it or who to report it to. Similarly, the research shows us that if staff cannot define a behaviour (e.g. deciding whether it is a security risk or a welfare issue), they are less likely to report it.
- The key message is for staff to trust their instincts – behaviours are often not black or white enough to be categorically defined on a checklist as 'unusual or unexpected'.

Emphasise the outcomes

- Unusual and unexpected workplace behaviour is often linked to a personal or workplace issue which could negatively affect the wellbeing of the individual and those working around them. By definition, insider behaviour causes harm to the organisation and/or staff members, but the potential repercussions are not always understood by staff. The consequences for the individual, team and organisation are set out in the diagram below:



Individual

- Increased workload
- Endangered security of personal information
- Less potential for a payrise or bonus
- Reduced job security

Team

- Increased pressures on the team/site
- Increased suspicion on the team/site
- Reduced security for the team – e.g. in one UK organisation, a whole team was disbanded due to a single insider act

Organisation

- Loss of customer trust
- Reputational damage
- Reduced profit/productivity
- Increased security/audit costs
- Reduced financial stability, etc.

Adding training content to existing initiatives – if there is reluctance to put staff through another training initiative, you should consider whether the messages from the staff training can be bolted on to existing training. It would work well with the following themes: security, staff wellbeing and welfare, health and safety, business ethics, etc.

The training aims will be shaped by what type of existing training (or other initiative) is selected as the forum. For example, you might consider the following:

Security induction training

Team briefings

Cyber security awareness

Wellbeing initiatives, e.g. Stress awareness

Self referral schemes

HR consultation

Toolbox talks

Team briefings

Health & safety induction

The staff training materials are purposefully generic, designed for all employees (and contractors), even managerial staff (additional training recommended – see 'Checklist' on pages 22–23).

Key elements to include:

- At least one scenario, preferably more
- Discussion of the behaviours following the scenario(s)
- Description of multiple options for how people can intervene/report
- How reports/information will be treated once collected
- Why people are being asked to intervene in unusual and unexpected workplace behaviour
- This will depend on the context, e.g. reducing potential for insider activity, looking out for colleagues (welfare), reducing financial and operational risk, because security is everyone's responsibility, etc.
- A contact point for trainees to refer questions, following the session

It is important to ensure that there is consistency between the 'It's OK to say' training and existing initiatives so as not to confuse any messages. It may also be asking a lot of staff and line managers to undertake more than one new initiative at once.

Induction training is another important avenue for 'It's OK to say'. Consider how new recruits will get the message that they shouldn't ignore unexpected and unusual behaviour in the workplace and at what stage in their induction.

Managing the implementation

Choose between local, centralised and third-party options – a major decision is whether the programme will be managed and rolled-out locally, or whether it will be disseminated from a single source. With regards to reporting channels, they are likely to be trusted more if they are managed locally, although conversely people may also be concerned for their confidentiality. In this situation, staff may have a preference for using a confidential helpline which is run by a third party.

With regards to rolling-out 'It's OK to say', it may be beneficial for the programme modules to be cascaded via managers in large organisations. They could then fine-tune the customisable components to make them more appropriate for the immediate context. This may be especially important for communicating reporting channels and tailoring training scenarios. In smaller organisations there is likely to be a greater understanding of the breadth and variation in job roles, as such a centralised approach to implementation may be more effective.

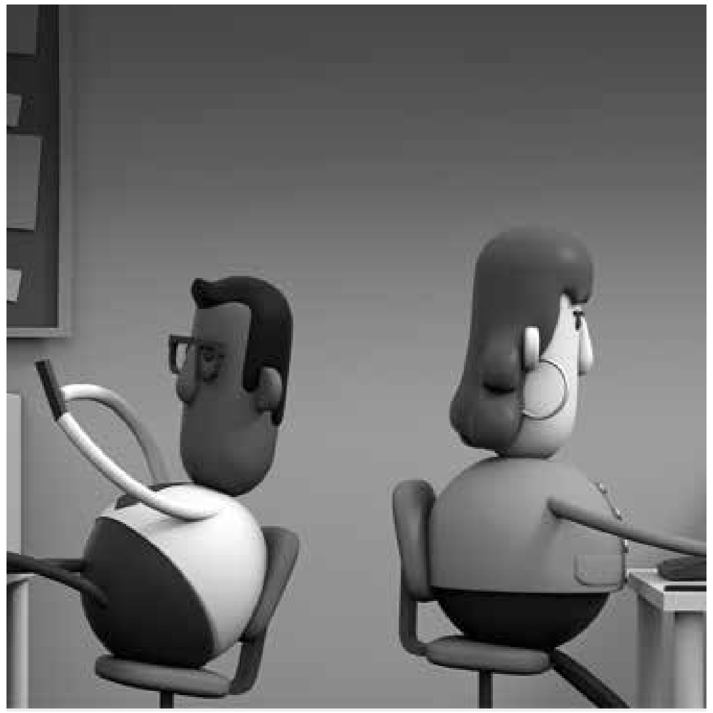
Explaining this programme to those who will receive it – the common message for staff, regardless of contextual alterations to the materials, is that they have a responsibility for themselves and those in their immediate work environment. There may be other particular reasons for why your organisation needs or wants to implement 'It's OK to say'. It is worth embedding these reasons in the rationale that staff will receive, in order to provide a tailored justification.

Furthermore, staff members may want to know why they are being asked to do this. In short, this is because they are likely to know their own environments and the people they work with better than people who are external to their teams.

Tailoring the programme to the organisation

Considerations for refining the programme: below we have listed some of the considerations for adapting the programme to the needs of your organisation.

- **Learning objectives:** 'It's OK to say' is underpinned by a set of learning objectives. Ensure these are in keeping with the messages you want to get across and existing related initiatives. This is set out in the 'Rationale for the programme' section (page 8).
- **Sequencing:** The communication materials are designed to provide both the 'warm-up' and 'follow-up' to staff training. If your organisation already has some form of insider threat awareness training or is planning a set of security campaigns which would provide context to these communications materials, then the materials may bolt onto that.
- **Resistance:** This is a sensitive topic for many staff. While they acknowledge security is important, they tend to believe that malicious threats to security reside only outside of the organisation. The animation is designed to introduce this topic in a light-hearted, entertaining way and therefore to essentially 'pave the way' for training.
- **Tailor training scenarios:** It is recommended that the scenarios for the staff training component of the programme are reviewed and key details are changed to reflect your organisation and the decided approach for implementing this initiative.
- **Pick and choose communications:** The posters depict different scenes from the animation, which can be selected to reflect the issues that your organisation may face. For example, a welfare or security perspective.
- **Substituting the animation:** If the animation is not considered suitable for your organisation it is still a good idea to provide some kind of 'warm-up' activity prior to training, especially for groups of trainees who are likely to be uncomfortable with the programme concepts. See next bullet for the 'Pre-training option'.
- **The 'Pre-training option':** This is essentially an interactive, trainer-led session, intended to raise awareness of the potential for insider activity within the workplace and prepare staff for training. The session is intended to include exploration of insider activity case studies, as well as group discussion focused on the potential for insider activity in trainees' workplaces. The group should include a few members who have some awareness of insider threat within the business or other involvement in security. The implementation of these sessions is recommended if particular resistance to the staff training is expected. Further information on the 'Pre-training option' and example group discussion questions is available on request. Case studies of insider activity from within the organisation will ideally be developed for the sessions.



- **Tailor the communications materials:** The posters and reminder cards allow you to add a logo and provide information about your organisation's options for staff intervention and reporting. These can be made relevant to specific business contexts if appropriate.
- **Repeat messages about intervention options:** Make use of the opportunities to clarify that there are multiple mechanisms in which people can intervene/report. Repeating the contact details of lesser-used channels (such as a helpline) is likely to be important in raising uptake.
- **Advertising the reporting process:** Ensure the programme clarifies how reports will be handled in terms of the six principles discussed under 'Ensure the mechanisms are fit for purpose" (pages 10–11). The staff training slides include two examples in the form of the 'reporting system principles' and 'Jackie the Helpline Operator'.

Post-programme

- Follow-up educational activities
- Evaluating programme impact
- Assessing the reporting system

Follow-up educational activities

Maintaining the 'buzz' – following the roll-out of the main programme, there is a risk the enthusiasm and learning gained from the educational aspects will fade. This is the point where post-programme activities play their most important role in refreshing people's memories and maintaining the 'buzz' around the programme, as follows:

- **Leveraging success stories:** Provide avenues for staff to learn of any success stories resulting from reports of unusual and unexpected workplace behaviour since the launch of the programme. Success stories need not include substantial detail (and they should certainly maintain individuals' anonymity and confidentiality) but demonstrate how, when and why someone decided to intervene in these behaviours, how this led to the identification of an issue and the positive outcomes that resulted. This will remind people about the programme and demonstrate that reporting is a worthwhile and socially acceptable endeavour. Various formats could be adopted, such as email, intranet postings or articles in the company magazine. As mentioned previously, the characters from the animation can be added to these communications to jog people's memories and maintain cohesion.

If there have not been any success stories so far, case studies of insider activities in other organisations could be utilised. These could point out where a colleague's intervention prevented an act or, as is the case with many publicised insider cases, where earlier intervention could have prevented various negative outcomes. Again this could be disseminated in any number of ways, for example a regular slot on the company intranet pages could be an effective means of keeping the central programme messages trickling through to all staff members.

- **Sending out reminders:** This could be a crucial time for drawing on your support network of 'champions' or 'programme ambassadors'. Consider whether it would be beneficial if one of these individuals were to relay a reminder of the programme messages or announce the successes of the programme. If someone holds particular sway with staff, publicising his/her endorsement could be very helpful for demonstrating how much support the initiative has received.
- **Publicising the evaluation:** Not only is the evaluation (see below) critical to establishing the successes to result from the programme, but it is important to communicate the results. This will help to renew enthusiasm and build further support.

All of these activities are expected to be instrumental in exerting a change in organisational culture, in which intervening when a colleague behaves in an unusual and unexpected way is widely considered the norm.

Evaluating programme impact

Defining what success will look like – when running a programme, it's important to know if it's working. This way, you can improve any shortcomings and build on successes. Programmes such as this aim to help improve the overall security culture and behaviours within an organisation. It should be evaluated to help measure this.

Below we have listed the initial considerations for developing an evaluation:

- How will you know if you have delivered against the objectives for the programme?
- What will you compare against? For example, a baseline or control group?
- What method will be used (e.g. questionnaire, interview, focus group)?
- What will be measured (e.g. awareness of behaviours and attitudes towards the insider threat, intention to intervene and actual reporting figures)?
- How many will be included in the evaluation activity and will you compare different staff groups?
- What timeframe will be used in order to measure effects (e.g. following roll-out, three months after)?

A suite of evaluation materials are available from CPNI to help with assessment of the training and communications elements.

Types of evaluation

Interim evaluation

People tend to think of evaluation activities as occurring at the end of the development cycle – to answer the question: 'does it work or not?' However, if you want to assess whether the educational components of the programme or reporting system are fit for purpose, an interim evaluation would be appropriate. This will help with tailoring the programme and identifying any problems prior to roll-out. One way to do this is to examine the plans and materials you have so far, looking to identify any issues and assess to what extent they meet the learning objectives. This review process is best carried out by a range of subject matter experts, for example:

- Training or communication specialists
- Contextual experts (e.g. control room staff if the context of a scenario involves a control room)
- Legal specialists (if legal connotations require assessment)
- Security managers and other individuals who will receive reports
- Members of the target audience

This review process is typically carried out on materials that are prototypes rather than final or near-final drafts. This enables them to be assessed and revised efficiently. Although interim evaluation may lengthen the development process, it reduces the possibility that the programme is implemented with flaws which will inhibit its success.

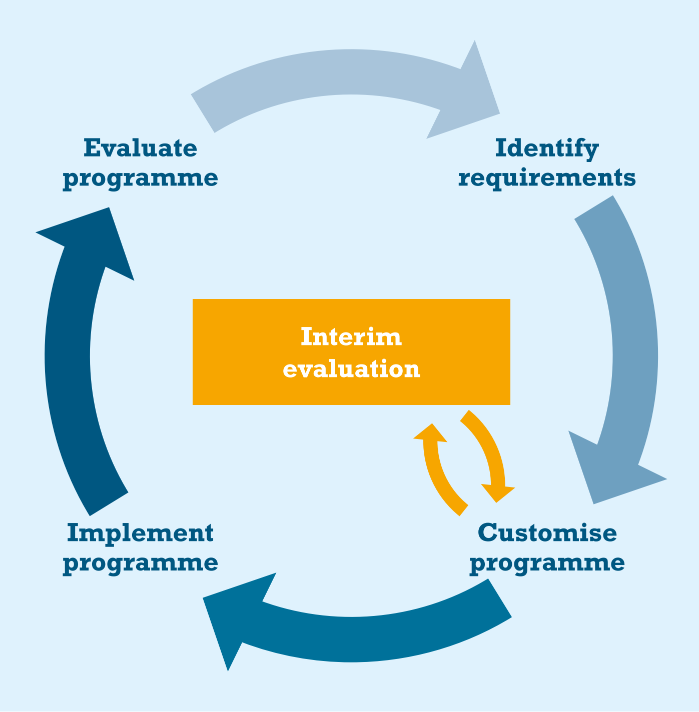
End-of-phase evaluation

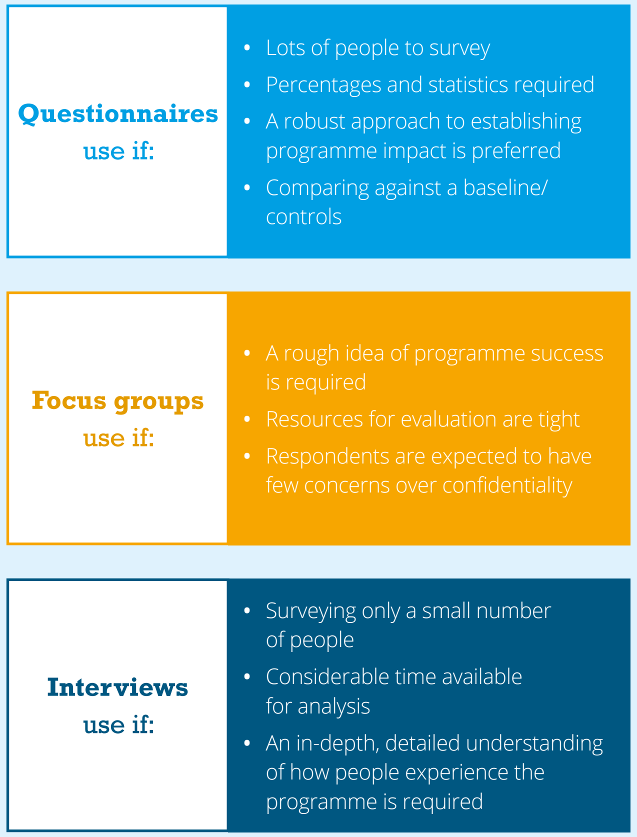
End-of-phase evaluation is more concerned with assessing how well a programme achieves its goals. This does not mean that it cannot also derive information about how to make improvements, but because it tends to be more resource-heavy than interim evaluation, it is sensible to conduct it on interventions that are more polished. The rest of this section will discuss considerations for evaluation in this traditional sense, i.e. evaluating the effectiveness of the 'It's OK to say' programme once implemented (at least within a section of the organisation).

Evaluation design – this section considers the decisions that should feed into the evaluation design process, as summarised in Figure 6 (Page 30).

What method to adopt

There are various options available; the most common methods for assessing a multi-layered programme are questionnaires, focus groups and interviews. Questionnaires are the most structured and easy to implement when the questionnaire is already designed. A focus group tends to involve less structure and encourages people to share their opinions amongst the group – much the same as the baseline workshops discussed on page 16. This is a good option if you would like to gain an impression of the perceptions and attitudes held by programme participants, including suggested improvements for future iterations of the programme. One-to-one interviews will be most viable if you only have a small group of participants and if there is concern about how honest they will be if interviewed as a group.





Questionnaires use if:
- Lots of people to survey
- Percentages and statistics required
- A robust approach to establishing programme impact is preferred
- Comparing against a baseline/ controls

Focus groups use if:
- A rough idea of programme success is required
- Resources for evaluation are tight
- Respondents are expected to have few concerns over confidentiality

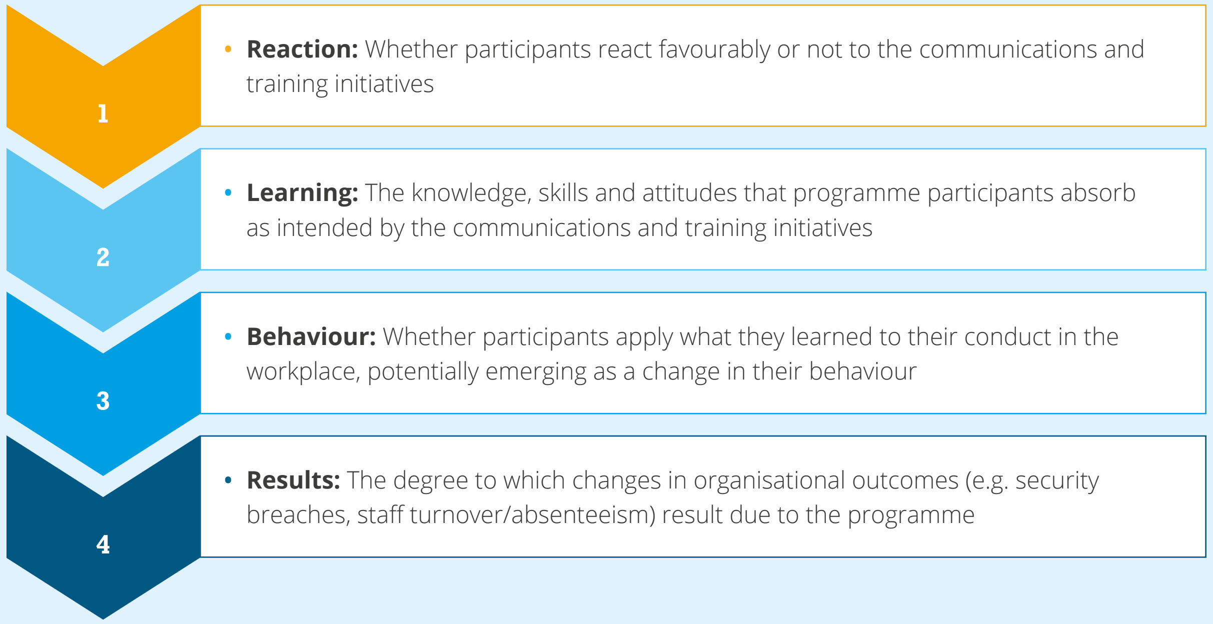
Interviews use if:
- Surveying only a small number of people
- Considerable time available for analysis
- An in-depth, detailed understanding of how people experience the programme is required

Figure 3: Research methods that can be used.

Some example interview questions which could be used for either focus groups or one-to-one interviews have been developed. The drawback to these methods is that they can require a great deal of time to undertake and the interpretation of the data can be complex and subjective. Questionnaires could therefore be the method of choice for evaluating the programme. An example set of both interview questions and questionnaires are available from CPNI.

What to measure

A commonly-used training evaluation model has implications for how the whole programme can be evaluated. Although it is probably not feasible to cover each of these four levels in depth, it shows the breadth of measures that would constitute an in-depth evaluation.



1
- **Reaction:** Whether participants react favourably or not to the communications and training initiatives

2
- **Learning:** The knowledge, skills and attitudes that programme participants absorb as intended by the communications and training initiatives

3
- **Behaviour:** Whether participants apply what they learned to their conduct in the workplace, potentially emerging as a change in their behaviour

4
- **Results:** The degree to which changes in organisational outcomes (e.g. security breaches, staff turnover/absenteeism) result due to the programme

Figure 4: The four levels of evaluation.

1 **REACTIONS:** The training department may already have a questionnaire that is used regularly to evaluate reactions to training. If this is the case, it could be beneficial to adopt this questionnaire for the purposes of consistency. As before, example questionnaires are available from CPNI.

2 **LEARNING:** Due to the nature of the programme, it will be difficult to design a formal assessment to measure the amount of learning, such as a knowledge test. It will be more meaningful to measure attitudes and perceptions of key knowledge relevant to the programme. Questions measuring learning should be linked to the learning objectives, as shown in Figure 5.

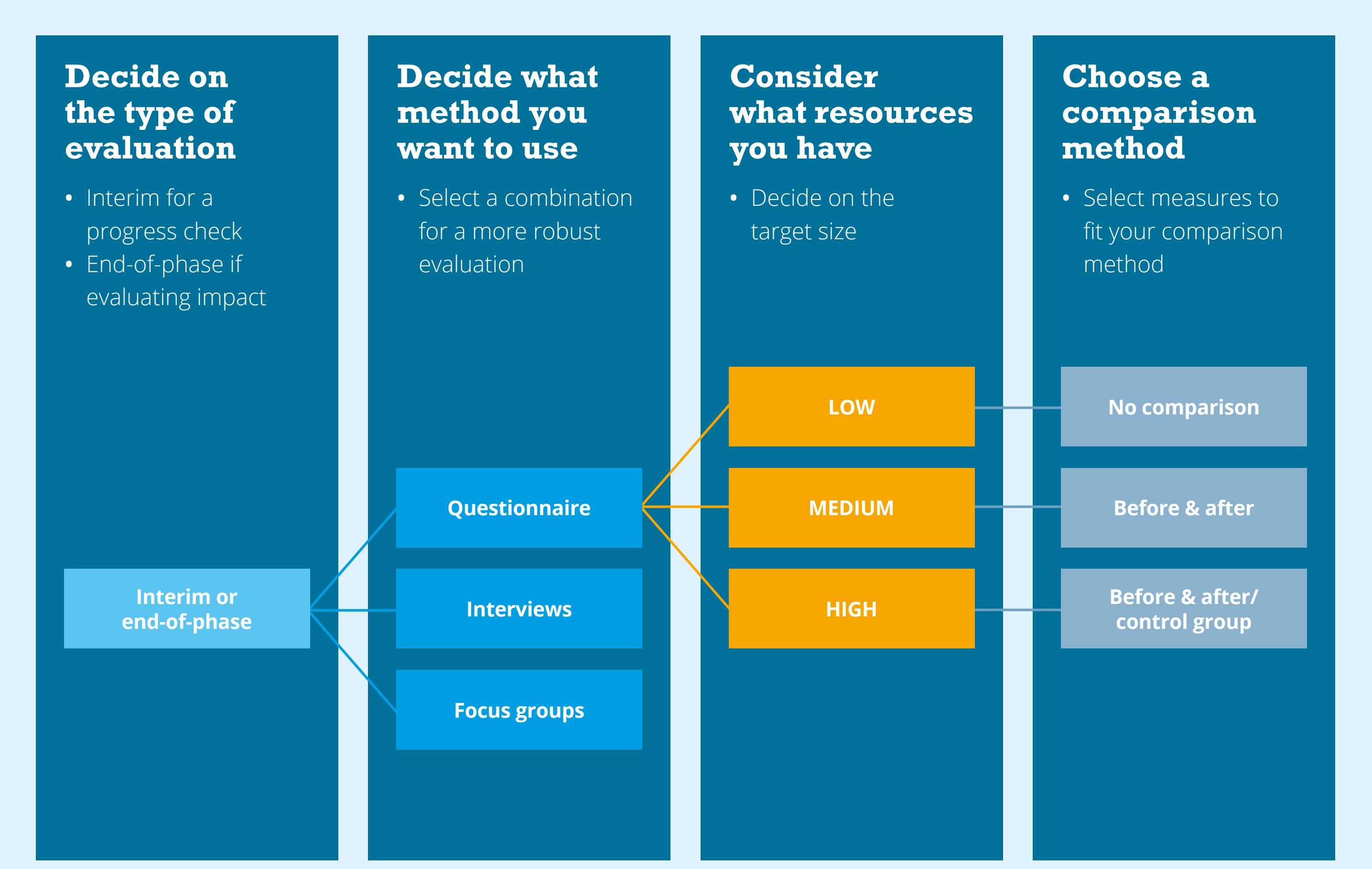
If additional learning objectives have been added to the programme, you will need to decide whether to develop more questionnaire items (which you could add to CPNI's questionnaire template - see Annex of Resources) or whether to assess them by post-intervention interview.

1) Improve understanding of the insider threat:				
How much do you understand about insider threat?				
□ Nothing	□ Very little	□ A little	□ A fair amount	□ A great deal
2) Improve awareness of unusual and unexpected workplace behaviours and their potential link with insider threat:				
How confident do you feel about recognising unusual workplace behaviours or activities?				
□ Very unconfident	□ Quite unconfident	□ Neither unconfident nor confident	□ Quite confident	□ Very confident
3) Enhance knowledge of how people can report or intervene when noticing these behaviours in the workplace:				
How aware are you of the ways in which you could report or intervene when someone is behaving unusually at work?				
□ Very unaware	□ Unaware	□ Neither aware nor unaware	□ Aware	□ Very aware

Figure 5: Example questionnaire items, relating to the learning objectives.

3 **BEHAVIOUR:** The ideal measure of the impact of this programme is whether or not people intervene following an observation of unusual and unexpected behaviour. This could include monitoring the individual, having a discreet conversation with a line manager, or reporting to a helpline. However, it is difficult to capture those types of intervention that do not involve making an official report to a specific channel. Very little information should be attached to official reporting figures in the interests of reporter confidentiality, so unless the programme is being rolled out across the organisation, it may be difficult to confirm whether a report is due to learning from the programme or not. CPNI has example evaluation questionnaires which depict a hypothetical situation towards which people's intended or expected behaviour can be measured. This measure is one way of capturing an impression of how the full range of intervention behaviours might be affected by the programme. It should be complemented by observations of reporting channel figures in order to gain an impression of actual reporting behaviour. One other suggestion is to include reporting of these types of behaviours into a 'red-team' trial that your organisation may run on insider threats. For example, if you intend to recruit 'insiders' in a scenario-based exercise plan, you might like to include interviews with colleagues/supervisors of those 'insiders' who may have been unaware that the exercise was taking place, in order to see if they made any reports and, if not, why they did not. CPNI has run insider threat 'red-team' exercises in the past and can provide advice on this if necessary.

4 **RESULTS:** This category of outcomes consists of the overall changes which have taken place and the impact that they have had. For example, if staff members have a greater tendency to intervene when they see a colleague behaving in an unusual and unexpected way, it could have benefits in terms of employee welfare, company security, team productivity, etc. Some examples for measuring results could be: the number of security breaches; staff turnover and absenteeism; costs incurred due to staff theft/damage; and levels of customer trust or confidence. However, these should always be treated with caution. It will not be easy to prove that these changes have directly resulted from staff members acting on the things they have learned in the programme. Furthermore, it will be essential to allow some time to pass so that the organisational outcomes of the programme can filter through. Nonetheless, this level of outcome is often the most important for justifying the resources spent on the programme and for future iterations of it.



Decide on the type of evaluation

- Interim for a progress check
- End-of-phase if evaluating impact

Decide what method you want to use

- Select a combination for a more robust evaluation

Consider what resources you have

- Decide on the target size

Choose a comparison method

- Select measures to fit your comparison method

Figure 6: A map of the key decisions to be made when establishing a design for evaluation activities.

Making comparisons

It can be very difficult to assess whether a programme has been effective or not by purely taking measurements following its implementation. Measuring both before and after the programme will allow the assessment of whether any changes have occurred in comparison to the baseline. This is helpful although not foolproof. In order to be able to assess whether the effects of a programme are entirely due to its implementation, it will be necessary to have a control group. These are people who are chosen because they are similar (in terms of their characteristics) to the group who have received the programme. They should be treated in exactly the same way as those receiving the programme although they do not receive the programme content. This is clearly challenging to achieve but will lend considerable weight to your evaluation. Alternatively, you could consider having a control group who receive the communications but not the training components. This will be helpful in establishing the benefit of training above the communications and therefore justifying the resource required to include training within the programme.

The decision to use a before and after design, with or without a control group, will be dependent on how much time the programme participants have and your own resources. Using a control group will mean 'denying' these individuals parts of the programme until you have completed your evaluation. This may or may not be feasible. You may decide that there will be no comparison method at all. This will affect how the questions are designed. A table of example items follows which incorporates the four levels of evaluation and how they might alter depending on the method of comparison adopted.

Level	No comparison	Before & after	Control group
1 Reactions	How would you rate the course overall?	Reactions cannot be sought from people prior to the programme	Reactions cannot be sought from people who haven't experienced the programme
2 Learning	To what extent has your confidence in recognising unusual workplace behaviours or activities improved as a result of this programme? (1) No improvement – (5) Vast improvement	How confident do you feel about recognising unusual workplace behaviours or activities? (1) Unconfident – (5) Confident	How confident do you feel about recognising unusual workplace behaviours or activities? (1) Unconfident – (5) Confident
3 Behaviour – Expected behaviour	Has the likelihood that you would intervene changed as a result of this programme? (1) Greatly reduced – (5) Greatly increased	In reaction to a scenario: What is the likelihood you would intervene? (1) Very unlikely – (5) Very likely	In reaction to a scenario: What is the likelihood you would intervene? (1) Very unlikely – (5) Very likely
3 Behaviour – Actual behaviour	Some comparison will be necessary to ascertain whether there have been changes in actual behaviour	Consider whether reports (e.g. to the helpline) have increased since the introduction of the programme	Consider whether reports (e.g. to the helpline) are greater amongst programme participants in comparison to non-participants
4 Results	Ask subject matter experts: Have you seen any changes with regard to security breaches since the programme was implemented?	Consider whether the number of security breaches has reduced since the rollout of the programme	Consider whether the number of security breaches is lower in the area of the business to receive the programme, compared to the 'control group' area

Table 1: Example measures based on the four levels of evaluation and comparison method

Practical evaluation issues

This section addresses some of the main issues that may arise during the course of carrying out an evaluation study.

Effects of the intervention over time

If the effects of the programme over time are of interest, it may be necessary to have more than one post-programme questionnaire. This can provide an impression of retained learning, although it is often essential to allow some time to pass before actual behaviour (Level 3) and the organisational outcomes (Level 4) can be measured. For the former, a period of several months is likely to be necessary, especially because the rate of unusual and unexpected behaviours may be quite low. It is advisable to allow a period of between six months and one year for organisational outcomes to filter through.

Managing the confidentiality of participants

Ensuring the confidentiality of those people who participate in the evaluation research is essential to gaining honest opinions and therefore valid information. In order to put people's minds at ease you should clarify how their information will be handled, who will handle it and what will happen to the information at the conclusion of the evaluation research activities. The procedures for handling the information should also comply with the Data Protection Act (1998).

Interpreting and reporting the data

The original design for the evaluation will help to determine what questions can be answered and the comparisons that can be made. For example, is there a difference between perceived knowledge about unusual and unexpected workplace behaviour before and after the programme in the direction expected? If so, this is evidence that this particular learning objective has been achieved by the programme.

Assessing the reporting system

After the reporting system has been functioning for a period, it may be advisable to assess whether it is fit for purpose, separately to evaluating the educational aspects of the programme. The reporting system could be assessed in the following ways:

- Reviewing feedback sheets from those who have reported. Feedback could be based upon the six reporting system principles. For example:
    - To what extent do you feel confident that your report will be kept confidential?
    - How satisfied were you with the post-reporting feedback you received?
- A comparison of reporting figures across different channels/time periods. Please note: it will be difficult to separate any interesting differences from staff members' awareness of the reporting system.
- A reiteration of the baseline workshops (see page 16) – in particular questions around the likelihood of reporting to particular channels.

Example evaluation plans

This final section outlines two plans for evaluating the programme: a 'rigorous' version, which is more resource-intensive but offers a more robust test of the programme and a 'light' version which requires less resources while still providing an indication of impact. You may choose to select elements from both plans and combine them on a single sample of programme participants, or you may choose to apply a more rigorous evaluation in some areas rather than others.

For this plan the following is recommended:

All participants to receive the programme should be surveyed if possible. If this is unrealistic, a representative sample should be sought. This should include a cross-section of the business areas and role types to receive the programme.

The following recommendations apply to both plans:

- A reasonable period of time should be allowed for measures of behaviour (Level 3) and results (Level 4) to be captured following roll-out.
- Reactions (Level 1) should be captured immediately after the training. This is harder to gauge for the campaign since posters and follow-up communications will be dispersed over time. It may be necessary to gather reactions to the campaign in two halves for this reason.
- The capturing of reporting figures should not necessitate the collection of additional demographic information (which is not normally required) because this could discourage people from reporting.
- Ethical and legal obligations relating to carrying out research within your organisation should be adhered to.
- Provision to assess the reporting system should also be made.

Rigorous evaluation plan

1 Reaction	• Level 1 reactions questionnaires – training & communications (all participants)
2 Learning	• Example questionnaires for thorough programme evaluation (all participants, compare pre & post programme/control group)
3 Behaviour	• Expected behaviour – example questionnaires for thorough programme evaluation (all participants, compare pre & post, etc.) • Actual behaviour – reporting figures (compare pre & post, etc.) • Survey line managers about off-the-record reports; survey HR/digital security etc. to capture perceptions of shifts in reporting
4 Results	• Carry out CPNI's SeCuRE Tool* before and after the programme to gain an understanding of shifts in security culture • Hold focus groups and/or interviews with senior project stakeholders about perceived shifts in high-level security factors • Track other organisational outcomes, e.g. security breaches

* SeCuRE is a survey-based tool which helps organisations develop a security culture strategy or clarify thinking about an existing security culture. It assesses employee perceptions about the way security is currently handled and helps to identify areas of potential risk. The results can be used by senior managers to help form the basis of a culture change programme.

Light evaluation plan

1 Reaction	• Communications questionnaires – training (survey all participants) and campaign (at least a representative sample of participants)
2 Learning	• Measure perceived changes in knowledge and attitude relating to learning objectives in a representative sample of participants; this info can be gathered by a questionnaire or focus group
3 Behaviour	• Actual behaviour – reporting figures (compare pre & post-programme) • Survey a sample of line managers about off-the-record reports, whether there has been a shift since programme implementation
4 Results	• Request brief opinion to a single open-ended question from senior project stakeholders to gather an impression of the shifts in high-level security factors since roll-out • Track quantifiable organisational outcomes, e.g. security breaches before and after programme roll-out

Annex of resources

Pre-programme

EVALUATION

- Guidance on conducting research – a short document containing tips and key principles
- Example scenario-based questionnaire
  - to gauge what employees might do if faced with particular scenarios and behaviours
  - to gauge perceptions around general organisational security
- Before and after questionnaire SET 1 – a set of scenario-based questions that can be issued to employees before and after the programme is run to gauge impact
- Before and after questionnaire SET 2 – a second set of the above

REPORTING MECHANISM

- Guidance on reporting system principles – a short document containing recommendations and key principles

Implementation

COMMUNICATIONS

- Animation (see storyboard pages 36–37) – for use as a warm-up to training
- Poster set (page 35 thumbnails) – for use post-training
- Reminder cards (page 38 thumbnails) – for use post-training
- Stickers (page 38 thumbnails) – for use pre-programme (as a teaser) or post-training (to remind)
- Animation stills – for use on intranet with organisation's own case studies

TRAINING

- Pre-training guide – a short document outlining suggested discussion topics for those who may be more resistant to the programme messages. For example, challenging perceptions around the insider threat
- PowerPoint slides for staff training session – slides, including trainer's notes and audio scenarios depicting unusual and unexpected behaviours' for discussion

Post-programme

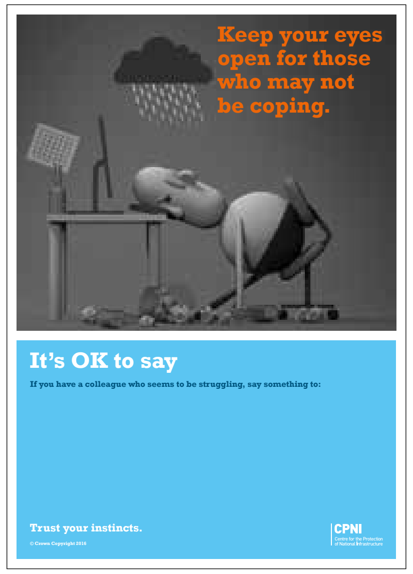
EVALUATION

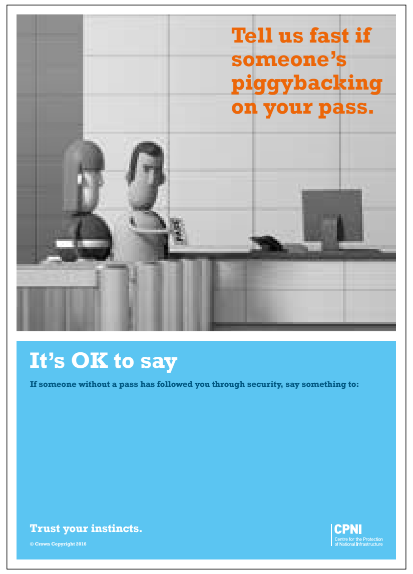
- Feedback questionnaire (communications) – a feedback form for employees to say what they thought of the communications (animation, posters etc.). Tailor according to products used
- Feedback questionnaire (training) – a feedback form for employees to say what they thought of the training provided
- Before and after questionnaire SET 1 – a set of scenario-based questions that can be issued to employees before and after the programme is run to gauge impact
- Before and after questionnaire SET 2 – a second set of the above

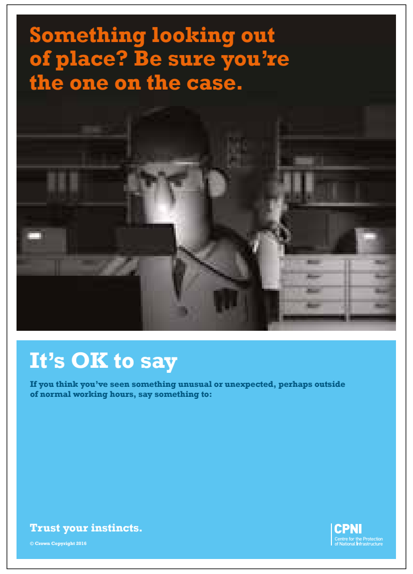
Other evaluation resources may be available on request to CPNI, for example for more in-depth studies to measure the impact of a programme.

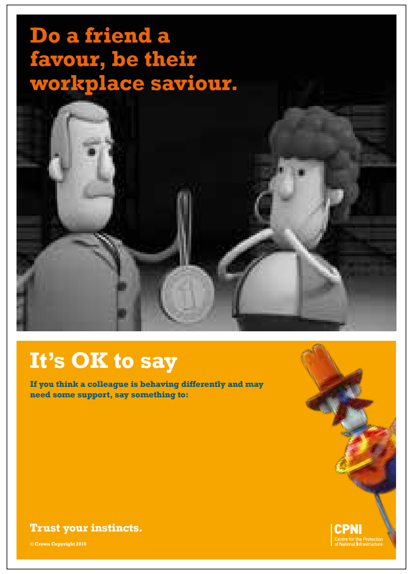
Posters

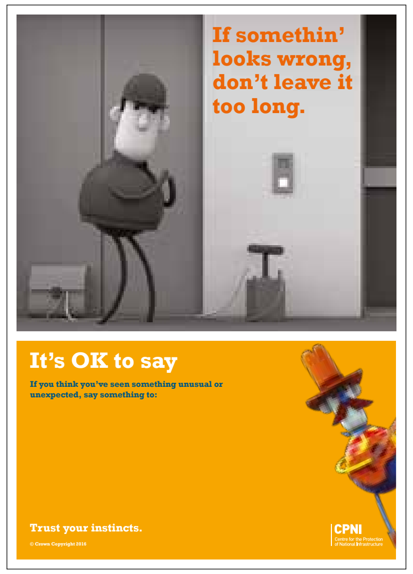
All designs shown are available in both colours.

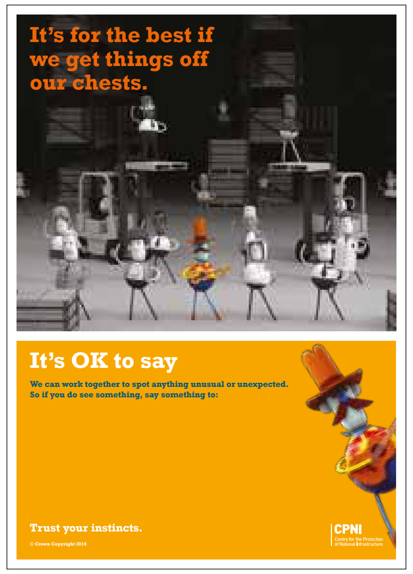

Keep your eyes open for those who may not be coping.
It's OK to say
If you have a colleague who seems to be struggling, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure

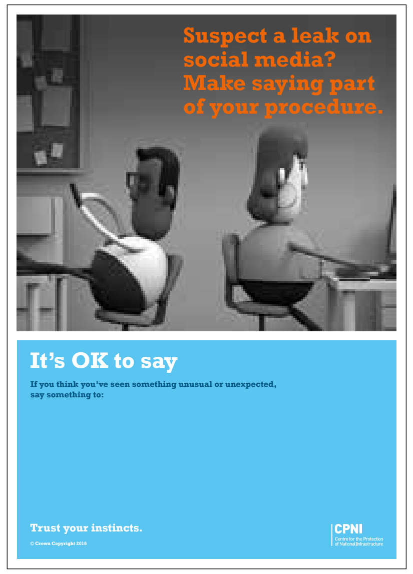

Tell us fast if someone's piggybacking on your pass.
It's OK to say
If someone without a pass has followed you through security, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure

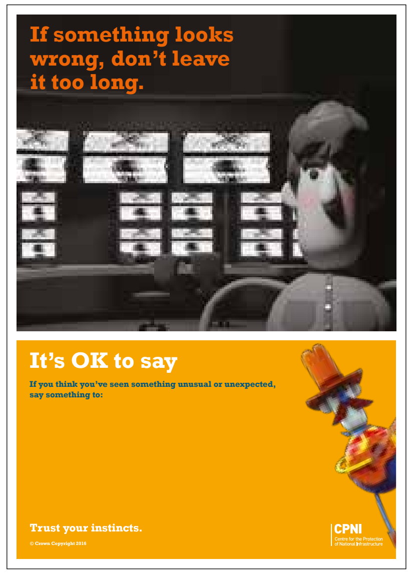

Something looking out of place? Be sure you're the one on the case.
It's OK to say
If you think you've seen something unusual or unexpected, perhaps outside of normal working hours, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure


Do a friend a favour, be their workplace saviour.
It's OK to say
If you think a colleague is behaving differently and may need some support, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure


If somethin' looks wrong, don't leave it too long.
It's OK to say
If you think you've seen something unusual or unexpected, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure


It's for the best if we get things off our chests.
It's OK to say
We can work together to spot anything unusual or unexpected. So if you do see something, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure


Suspect a leak on social media? Make saying part of your procedure.
It's OK to say
If you think you've seen something unusual or unexpected, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure

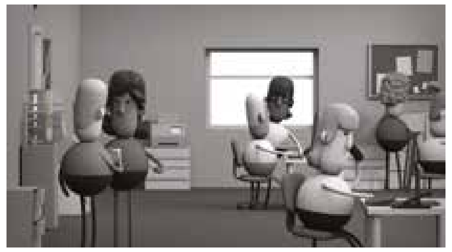

If something looks wrong, don't leave it too long.
It's OK to say
If you think you've seen something unusual or unexpected, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure

Animation storyboard

1

It's OK to say

2



3

This lil' song is here to instruct ya,
to help protect your infrastructure,

4

how to keep your workplace safe and sound.

5

'Cause there's times it's right to spot
some wrongs,

6

your hunch may be true all along,
if you've seen folk moseyin' around.

7

That guy with a rucksack by the lift, he
don't look familiar, looks kinda shifty

8

you don't want to say, you don't want to
cause a scene.

9

They might be a bit of a loon
and if you don't say something soon

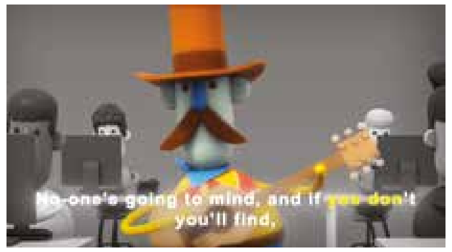
10

He could blow us all to smithereens.

11

It's OK to say, it's OK to say,
it's OK to say when somethin's wrong.

12



13

it could be Armageddon 'fore too long.

14

Bob's not right, he seems real strange
he ain't the same, there's been a change

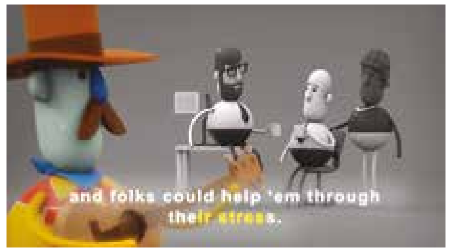
15

it could just be his life is in a mess.

16

So try and keep your peepers open
to spot someone who just ain't copin'

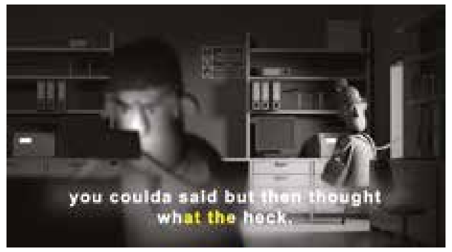
17



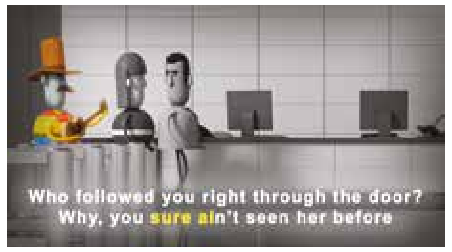
18

He's takin' pictures on his phone,
workin' late, and' all alone,

19



20


Who followed you right through the door?
Why, you sure ain't seen her before

21

so tell someone so's they can go
and check.

22

'Cause if you're too polite, you could get
a real big fright,

23

it's much safer if somebody checks it out.

24

She's fiddling with that guy's PC
sure looks mighty strange to me

25

but too late now 'cause
everyone's infected.

26

He's leakin' stuff on social media and
that ain't part of our procedure,

27

y' shoulda said as soon as you'd suspected.

28

It's OK to say, it's OK to say,
it's OK to say when you're in doubt,

29

So we're asking you to keep alert 'n
check things out if you're not certain

30

chances are it ain't nothing at all.

31

You might be doin' a friend a favour
end up being the workplace saviour

32

if you simply make a little ol' call

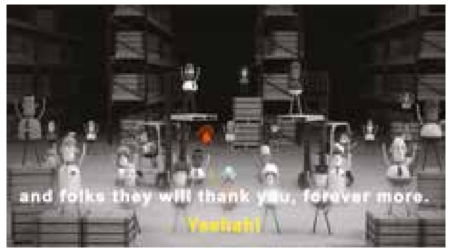
33

It's OK to say, it's OK to say,
it's OK to say when you're not sure.

34

So get it off your chest,
it'll work out for the best

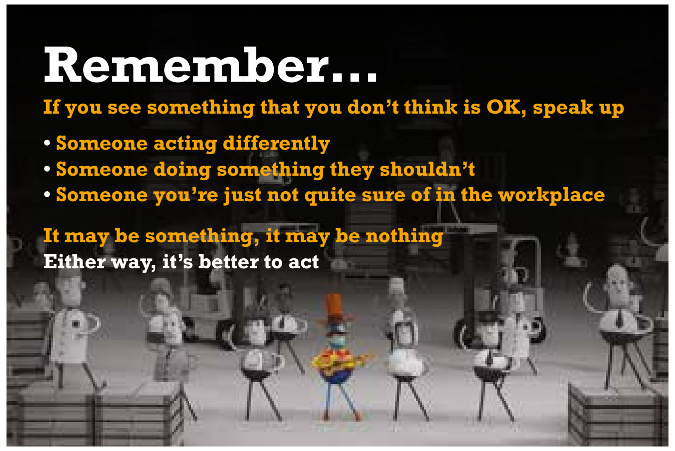
35



36

If it looks unusual,
trust your instincts.
It's OK to say.
CPNI
Centre for the Protection of National Infrastructure

Reminder cards

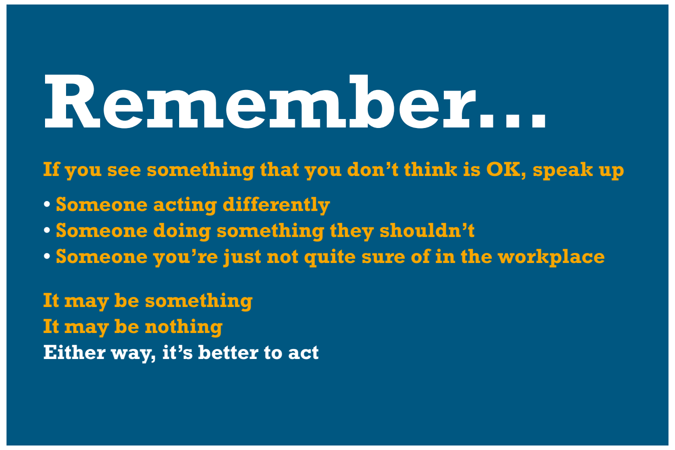


Remember…

If you see something that you don't think is OK, speak up

- Someone acting differently
- Someone doing something they shouldn't
- Someone you're just not quite sure of in the workplace

It may be something, it may be nothing
Either way, it's better to act

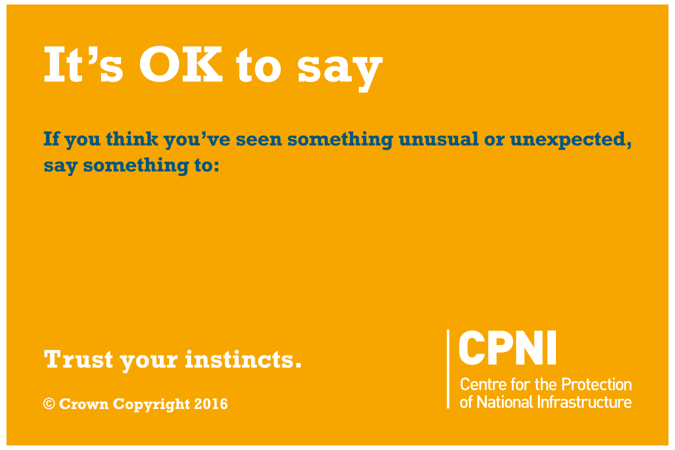


Remember…

If you see something that you don't think is OK, speak up

- Someone acting differently
- Someone doing something they shouldn't
- Someone you're just not quite sure of in the workplace

It may be something
It may be nothing
Either way, it's better to act



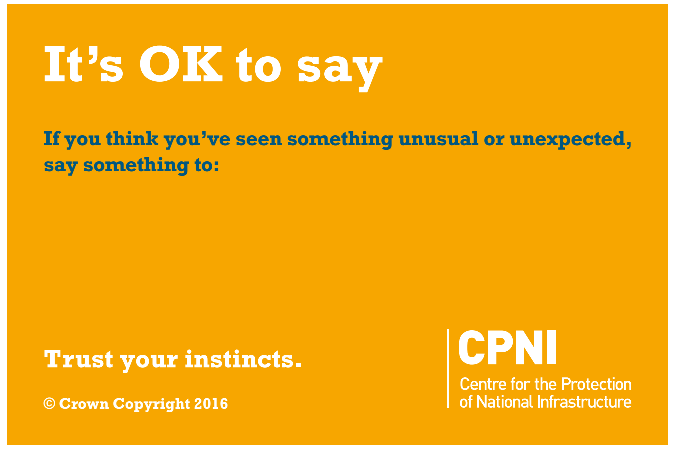
It's OK to say

If you think you've seen something unusual or unexpected, say something to:

Trust your instincts.

CPNI
Centre for the Protection of National Infrastructure

© Crown Copyright 2016



It's OK to say

If you think you've seen something unusual or unexpected, say something to:

Trust your instincts.

CPNI
Centre for the Protection of National Infrastructure

© Crown Copyright 2016

Window stickers

CPNI
Centre for the Protection
of National Infrastructure

It's OK
to say
CPNI
Centre for the Protection
of National Infrastructure

Notes

CPNI

Centre for the Protection
of National Infrastructure