



General Data Protection Regulation (GDPR)

Privacy and Data Protection

General Data Protection Regulation (GDPR) requires us to adopt a ***privacy by design*** approach ensuring information security, privacy and data protection is embedded in the processes and ways of working across the organisation.

A key aspect of this is ensuring there is sufficient awareness and training of the issues for all staff and volunteers.

The information and material in these slides will ensure all of us within CAFOD have a basic, common understanding of practical things we should know and do to protect the data and information that is now so pervasive in all our work.

In the interest of stewardship and costs, these slides are presented largely unedited from the originals provided under free license by HM Government.

Responsible for Information

This course is for **CAFOD Staff & Volunteers** who handle information and need to process, store and share this information in a secure manner. It will help improve your knowledge and understanding of information security.

The course is divided into six topics:

- **Definition of information and information security**
- **Protecting and sharing information**
- **Information in the workplace**
- **Working on the move**
- **Staying safe online**
- **Fraud**


It is recommended that you work through the course from start to finish, although you can complete the course in stages if you prefer.





Definition of information and information security





Information is vital to CAFOD. Without information the organisation cannot function. Therefore, it is necessary to protect and safeguard information, in particular confidential and sensitive information.



What is information security and why do you need it?

Definition of information and information security

What is information?

Information is something that has meaning. But what is the meaning of information and information security?

The Oxford English Dictionary defines **Information** as: Facts provided or learned about something or someone. The imparting of knowledge in general.

The practice of protecting information is information security.

The ISO/IEC 27002 defines **Information security** as: The preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information must be protected when transmitted, stored and during processing.

Definition of information and information security

Information security definitions

The ISO/IEC 13335 standard defines the confidentiality, integrity and availability properties of information security as detailed below:

- **Confidentiality:** information is not made available or disclosed to unauthorised individuals, entities, or processes
- **Integrity:** safeguarding the accuracy and completeness of information assets
- **Availability:** information is accessible and usable upon demand by an authorised entity



Definition of information and information security

The importance of information security

The processing, storing and retrieval of information is critical to all organisations.

In commerce:

- After major security breaches only 21% of businesses implemented additional staff training and communications to protect against the human risk in cyber security. 20% of businesses took no actions to prevent and protect their organisations from further breaches.
- 65% of large firms detected a cyber security breach or attack during 2016. 25% of these experienced a breach at least once a month.
- the average total cost to a small business of its information breaches over 2016 was £3,480.
- Only 35% of Britons are following the latest advice from Government to use strong passwords made up of three random words.

These slides will provide an introduction to information security concepts.



Protecting and Sharing Information

Protecting and sharing information

Accessing information

All information needs to be accessible when required, with unauthorised access and modification prevented. In addition, sensitive information needs to be kept secure and confidential.

Information has different classifications, some information may be sensitive or confidential, other types of information could be unclassified. The products and services supplied by an organisation would be unclassified (for public consumption).

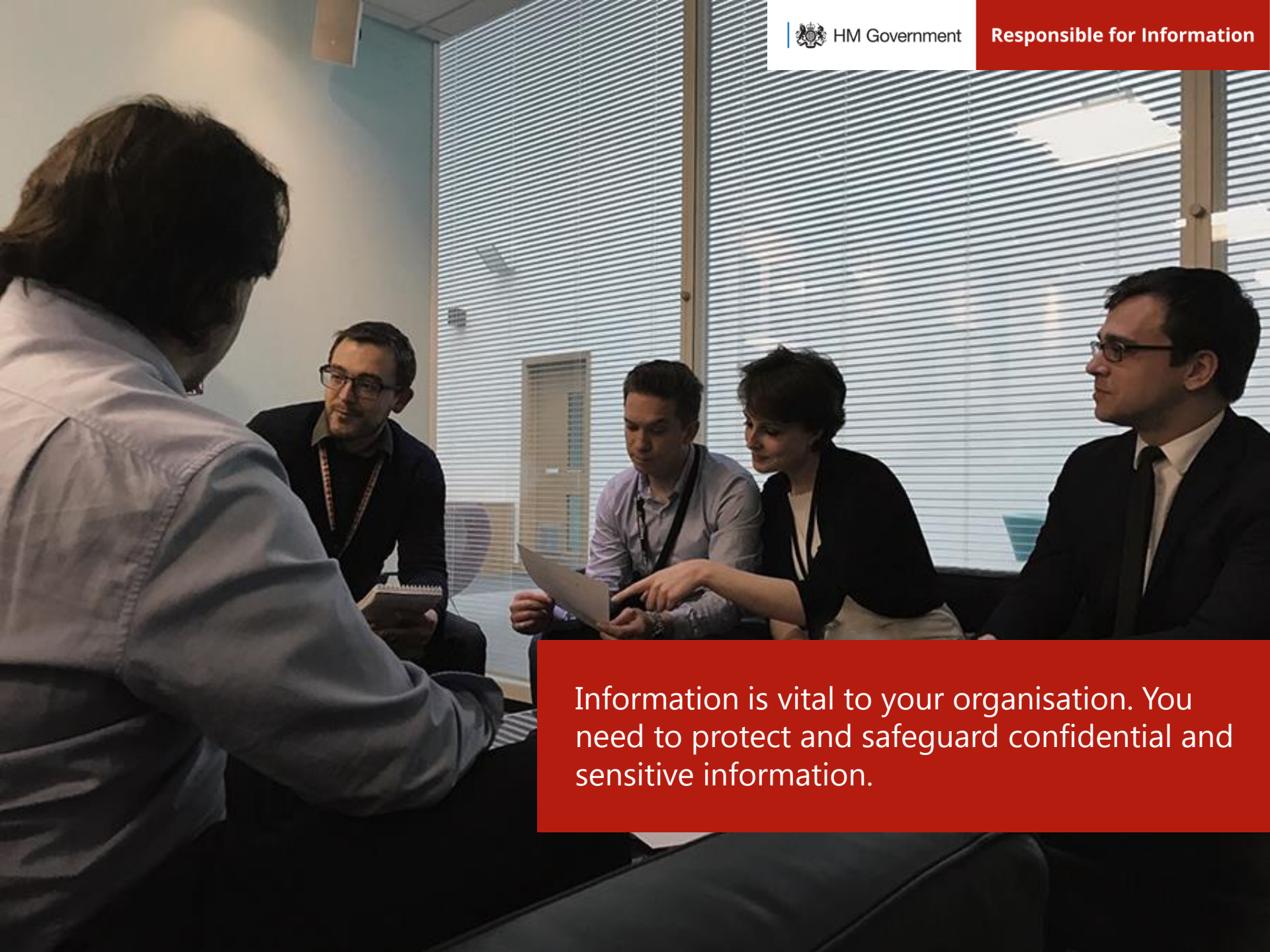
However, information considered as the intellectual property of an organisation would need to be protected.

Protecting and sharing information

People, processes and technology

People, processes and technology are important components of information security. Through recognition, identification and implementation, these controls will improve the organisation's ability to mitigate information security risks. Each component consists of a number of attributes as detailed below:

- **People:** Culture and attributes, skills and training, organisation, roles and responsibilities
- **Processes:** Ensure applications, architecture and infrastructure components are correctly identified, recorded and documented. These components need to be installed and configured correctly, updated, monitored and recorded. The necessary security controls and mechanisms also need to be implemented
- **Technology:** Ensure the necessary procedures, standards and regulatory requirements are correctly defined, documented, published, implemented, monitored and recorded. An ongoing improvement process should also be implemented. This will provide a mechanism to allow the organisation to develop and improve further



Information is vital to your organisation. You need to protect and safeguard confidential and sensitive information.

Protecting and sharing information

Types of information at work

Take a look at the three **types** of information you may find in your organisation:

- **Supporter & Volunteer information** is information about **supporters and volunteers**, such as their name, contact name, address, telephone number or bank account details. It may also include donation / order details. Some of this information is particularly sensitive. **All information** about individual people needs to be treated with care.
- **Intellectual property** includes trade secrets, a formula, design, instrument, patents, products, industrial or design rights, these need to be protected. Other types of intellectual property also exist including, copyrights, trademarks and trade dress. However, these would not normally need to be kept confidential
- **Organisational and operational information** may include standard operational processes such as programme controls and management, invoicing, purchasing, processing orders and other internal processes

Protecting and sharing information

Why information is critical to your organisation

Without information your organisation simply cannot function, it's the lifeblood of the organisation. Information is an **asset**, just like your supporters, property, materials, equipment, vehicles or money. It enables the organisation to deliver its mission. Therefore, you need to protect supporter and volunteer information, intellectual property (IP), organisation transactions and operational processes and procedures.

Organisations store, process and transfer supporter information every day. This may include confidential payment information from debit or credit cards. Organisations are required by law to protect payment card information as detailed in the Payment Card Industry Data Security Standard PCI-DSS.





Information comes in many types and formats.

Protecting and sharing information

Where is information physically located?

Information can be electronically stored, processed and transferred by various mechanisms and devices. These physical devices store or transfer the information detailed on the previous two slides. A staff member or volunteer requires a physical device to access, store and transfer this information. These devices come in different formats as detailed below:

- Laptops and notebooks
- Workstations
- Smartphones
- Tablets and PDAs
- Storage devices (hard drives and USB pens)
- Servers
- Networks (during information transfer)
- Cloud

Information can also be stored physically in the form of paper documents.

Protecting and sharing information

Logical location of information

Information is located across organisations and contained in different file formats and stored on physical devices. The list below identifies the files, software and applications used to create, manage, manipulate, retrieve or delete information:

- Staff/volunteer files (documents, presentations, spreadsheets, images and sounds)
- Emails (stored on the CAFOD network and on internet based services)
- Websites including social media (Twitter and Facebook)
- Databases (personnel, supporter database)
- Metadata (data about data)
- Smartphone applications (mapping software)
- Applications (word processors, CRM (CSD) and document management systems (SharePoint))



Protecting and sharing information

Classifying information

Different information has different classifications. The Information Asset Owner (IAO) of the organisation would normally be responsible for assigning a classification to the information based on the organisation's information classification system.

The following general list provides examples of different information classifications:

- **Very High Sensitivity or Secret**
 - Intellectual property critical to the success of the business
 - Medical records, sexual orientation or political views
 - Employee salaries or remuneration packages
 - Payment information such as credit card details
- **Highly Sensitive or Confidential**
 - Personnel records, detailed financial records
- **Medium Sensitivity or Restricted**
 - Business processes
- **Low Sensitivity or Unclassified**
 - Publicly allowed finance information (annual returns)
 - Product prices, activities or services provided

Protecting and sharing information

Classifying information



Within CAFOD, we will use three, simpler classifications of information:

Public: This information is not particularly valuable, nor is CAFOD required to protect it. It can be accessed by anyone for any purpose, including release to supporters, volunteers or the general public. It may include press releases, job vacancies, etc.

Internal Use Only: This information has value internally, and may have some value to other INGO's. It may be distributed freely to anyone within CAFOD but not to others outside the organisation. It may include internal memos, employment data, contract information, and so on. This is the category where the clear majority of CAFOD's information will reside.

Confidential: The information has significant value and there may be legal requirements for its protection. Access is limited to designated roles or tiers within CAFOD. It may include personal information, intellectual property, financial information, long-term strategic planning, and so on.

How you handle information is very important. Supporters & Volunteers have entrusted their information to you. If you misuse or lose personal information it could cause serious harm or distress to people.



Protecting and sharing information

When information is not handled carefully

If organisational information is compromised either through deliberate (internal or external) or accidental (internal) threats, serious consequences to the future operation of the organisation may be affected.

This may be permanent or at least long-term. Information compromised either through loss, leakage or theft could impact an organisation's financial position and/or damage its reputation. Supporters and other stakeholders may no longer trust the organisation.



Protecting and sharing information

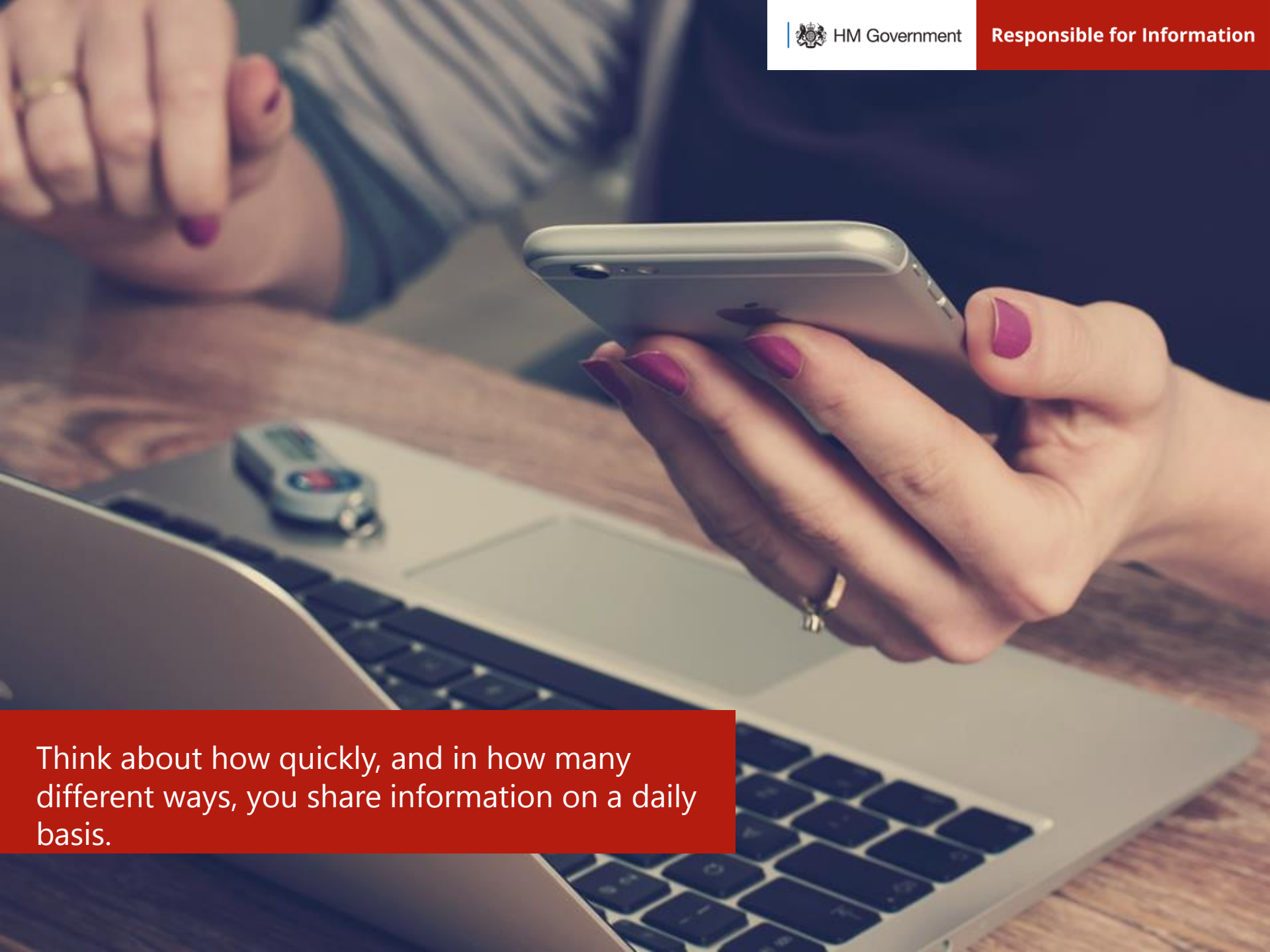
Information and you

Whatever type of information you create or handle, you are entrusted to look after it. Information is **your** responsibility.

You are responsible for **all** of the following:

- Information about yourself
- Information about your organisation
- Information about your colleagues
- Information about your stakeholders (e.g. supporters, volunteers, donors, beneficiaries)





Think about how quickly, and in how many different ways, you share information on a daily basis.

Protecting and sharing information

It's important to share

Take a look at how you can work more efficiently simply by effective information sharing.

Claire's team has just started a new project with a customer to design and build environmentally-friendly office buildings. Claire's company is acting as project managers.

Due to recent organisational changes, Claire's team doesn't have the details of the necessary environment constraints for the area and a full survey of the plot. This means the team will have to complete a survey and obtain the necessary environmental information. This takes a lot of time and resources.



Protecting and sharing information

It's important to share

Take a look at how you can work more efficiently and effectively through simple information sharing.

Claire meets Simon, who works at a local architect firm, and discovers he has worked with other organisations on previous projects with similar requirements. He already has details of the required components to complete an environmentally-friendly office build.

Simon checks with his line manager that the information can be shared and then sends it to Claire's team.



Protecting and sharing information

Consider the outcomes

Clearly, information sharing can be hugely beneficial. For example:

➤ **Time and money are saved**

It would take significant time and resources to gather the required information. By re-using previous information, Claire's project is ahead of schedule

➤ **Previous research is given new value**

Simon and his team are pleased that the work that they previously carried out continues to have value. This is motivational and underlines the importance of their daily work

➤ **Relationships are built**

Simon and Claire's information sharing has strengthened the relationship between the two companies, should they need to collaborate in the future. In short, they have established a firm connection based on productive information sharing

In CAFOD's context – think of sharing information about designing a project or programme with a sister agency or other INGO

Protecting and sharing information

Share with care

It is crucial to **respect** the information that you share, as it can affect people in many ways.

I'm Julie. I had to take time off work for a medical emergency. I was off work for two weeks, so had to provide hospital and doctor's notes.

I'm Julie's line manager, Harmeet. I helped Julie back into work and passed on the medical information that Julie gave me.

I'm Alex, the welfare officer. I dealt with the information that Julie's line manager gave me. I asked Tom to help me with the filing as he's new to the department.

I'm Tom. I helped with the filing. I mentioned Julie's condition to my good friend John. He had the same condition last year.

I'm Arup. My friend Emma happens to work with Julie. We talked about Julie's condition and I passed on my sympathies through her. I know how difficult the condition is to deal with.

I'm so mortified that everyone knows about my condition. I never wanted it out in the open and feel like everyone is talking about me



Protecting and sharing information

Think, check, share

Before sharing information, consider the following actions:



➤ **Think**

- What's the information about?
- Is this information sensitive?
- Who am I giving this information to?
- What is it going to be used for?
- Do I have permission to share this information?
- Is it legal to share?
- Am I only sharing what I need to?

➤ **Check**

Check if the information that you want to share is in line with your organisation's policy.

➤ **Share**

If you've analysed and checked the information you should be in a position to share it.

Protecting and sharing information

Considering security

Security is important. Look at the example here.

Joy has been asked to send photocopies of some work contracts to Iain in another department. These contain personal information including salary details. She puts the copies in an envelope and places it in the office post tray for next day delivery.

Three days later, Iain calls Joy to say he has not received the contracts. Joy lets him know that she will look into it. Since she sent it by regular post, there is no way she can track it, so she sends another copy immediately, this time through recorded delivery.

Iain receives the second set of contracts the next day. The first envelope never reached him and Joy never thought to mention the loss to anybody else.



Protecting and sharing information

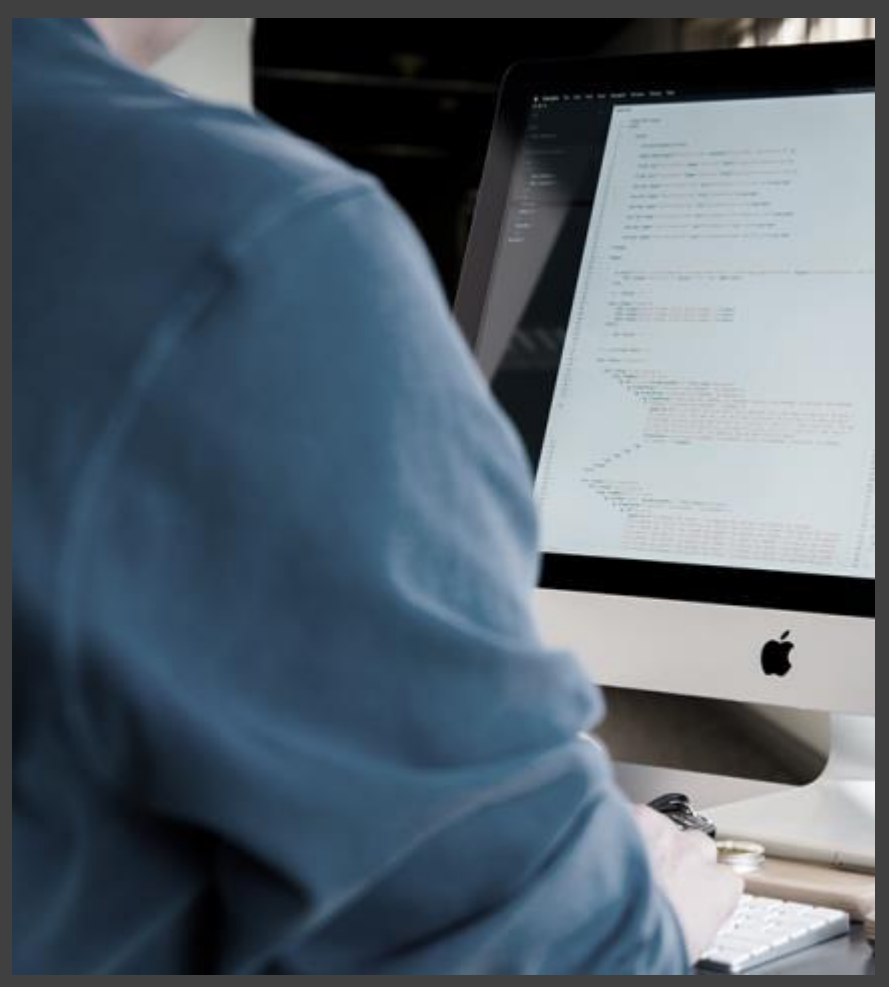
What went wrong?

Security is important. Look at the example here.

Joy should have reported the loss and should have chosen a secure method to send the information.

Joy made a few important mistakes. The people whose contracts were lost in the post would have been upset to find out their personal details were mislaid and ultimately it may have had more serious consequences.

Always make sure you check your organisation's policy on how to share information securely.





Sharing needs to be done securely. Check your organisation's policy. If in doubt, ask.

Protecting and sharing information

Summary

Let's recap the key points:

- Information is vital to your organisation
- Information can come in many types and formats
- You need to protect it
- You need to be able to share information according to your organisation's policy
- Sharing information can have huge benefits, if done correctly
- Mishandling information can cause harm and distress
- Think and check before you share





**Information in the
workplace**

Whatever your organisation or work environment looks like, you are responsible for protecting information.

Information in the workplace

Risks in the workplace

The workplace can contain many information risks.



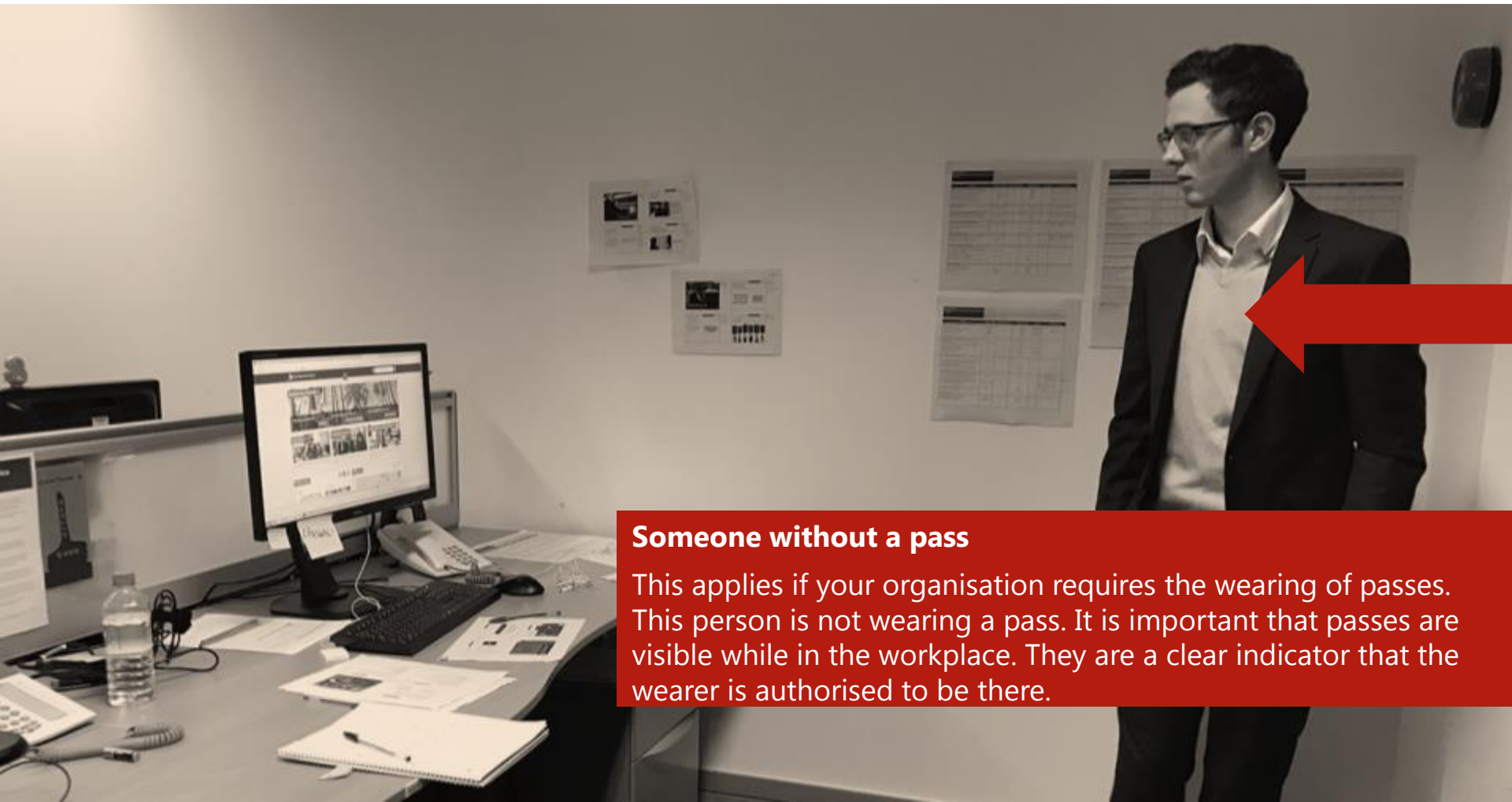
Passwords on post-it notes

Passwords should never be shared or left on display. Passwords ensure that only the right people have access to information.

Information in the workplace

Risks in the workplace

The workplace can contain many information risks.



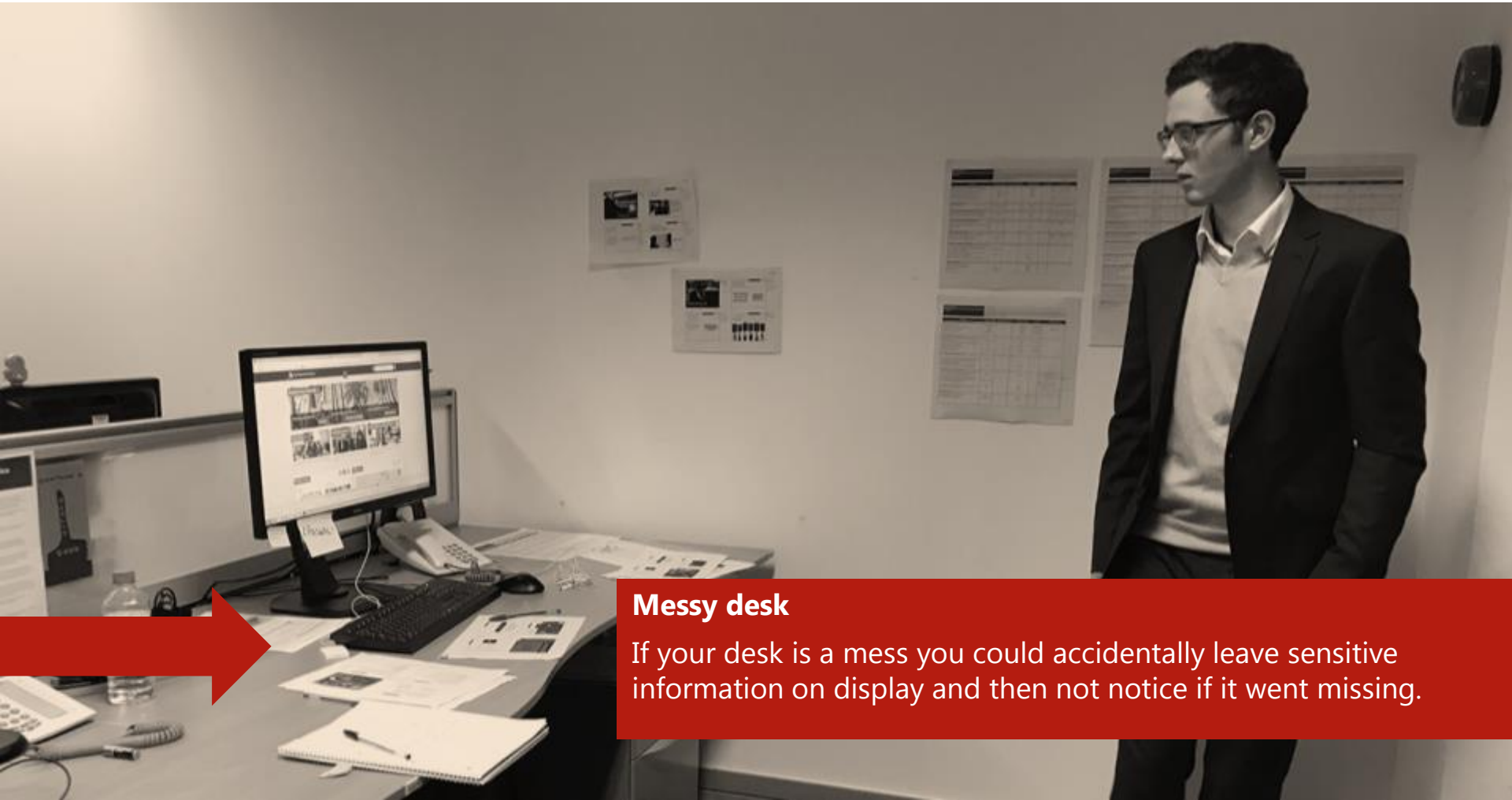
Someone without a pass

This applies if your organisation requires the wearing of passes. This person is not wearing a pass. It is important that passes are visible while in the workplace. They are a clear indicator that the wearer is authorised to be there.

Information in the workplace

Risks in the workplace

The workplace can contain many information risks.



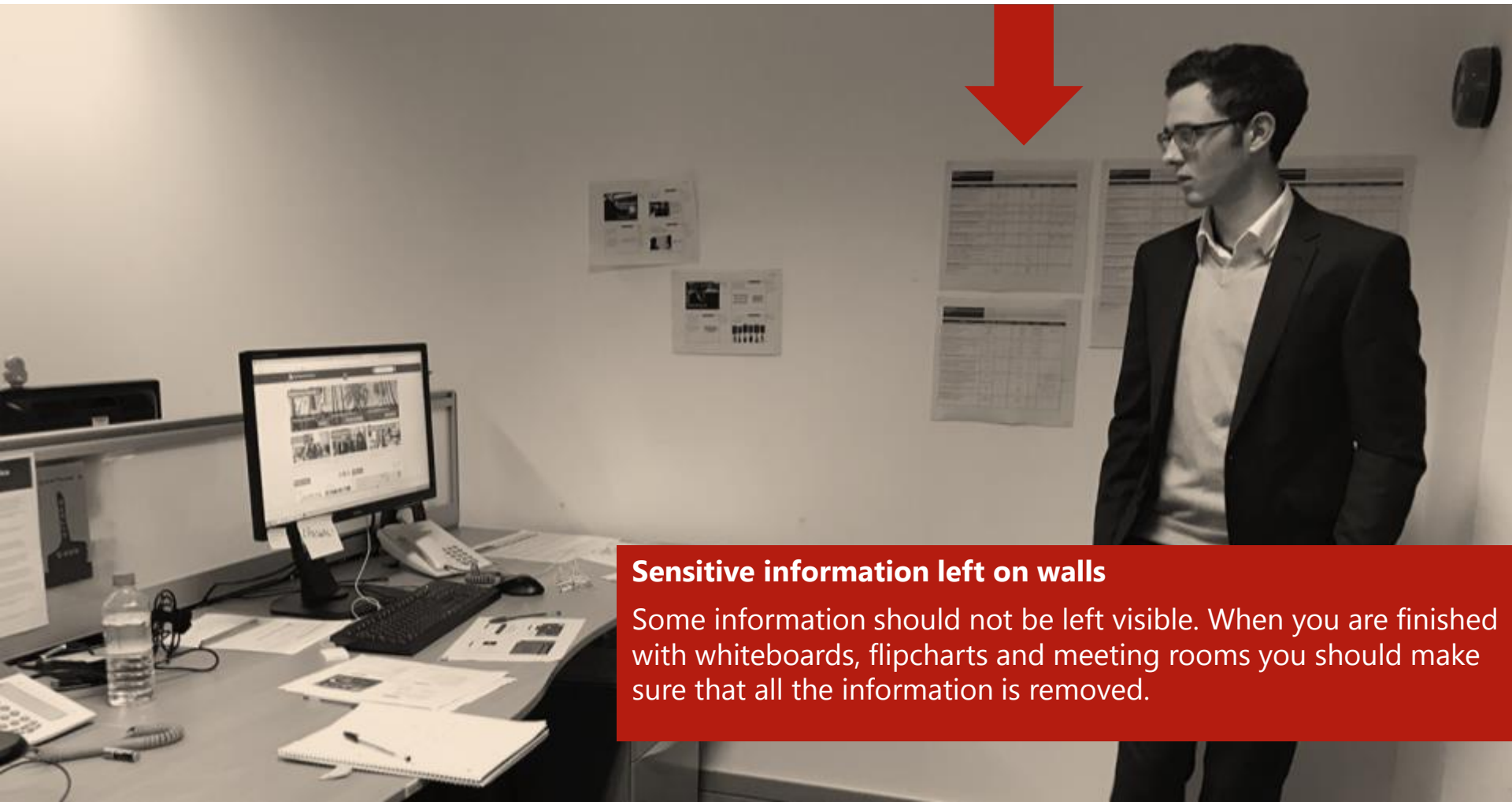
Messy desk

If your desk is a mess you could accidentally leave sensitive information on display and then not notice if it went missing.

Information in the workplace

Risks in the workplace

The workplace can contain many information risks.



Sensitive information left on walls

Some information should not be left visible. When you are finished with whiteboards, flipcharts and meeting rooms you should make sure that all the information is removed.

Information in the workplace

Risks in the workplace

The workplace can contain many information risks.



An unlocked computer

This computer has been left unlocked. Make sure you lock your computer when it is unattended to prevent unauthorised access. This protects the information and safeguards you from blame if the computer is misused while you are away.

Information in the workplace

Risks in the workplace

The workplace can contain many information risks.



Sharing passwords

There is a tendency to share passwords in the workplace because of trust and familiarity between members of staff. Don't share passwords with other people because of the information related risks.

A black and white photograph showing a person's hands operating a shredder. The shredder is processing a stack of papers, with shreds falling into a collection tray. The scene is focused on the mechanical action of the shredder and the hands of the operator.

Make sure you protect and dispose of information correctly.

Information in the workplace

Cutting corners

Consider the example below:

Therese's boss, Justin, works remotely in the field conducting water surveys. Today he needs some specific client information before his site visits. He contacts Therese and asks her to send him the information.

Therese knows that to externally log onto the organisation's intranet involves a long registration process, so she emails the spreadsheet containing the client information to Justin's work and personal email account.



Information in the workplace

Cutting corners

Consider the example below:

Therese receives a call on her mobile phone from her neighbour downstairs. She has limited mobile reception in the office, so she walks outside to take the call.

Without thinking, she leaves her computer unlocked. The client information she has been working on is still open.



Information in the workplace

Cutting corners

Consider the example below:

Her neighbour informs her that water seems to be leaking from a pipe in her kitchen and has started to trickle through to his ceiling. As she is about to leave to go home, she remembers she has left documents by the printer and asks her colleague Alice to pick them up for her.

Alice happily obliges, but doesn't realise that she hasn't collected all the printed documents. These get left by the printer and eventually get thrown in the recycling bin by the cleaners.



Information in the workplace

Consider the outcomes

What are the possible consequences of Therese's actions?

- **The email to her colleague could be intercepted on the internet**
Never use personal email accounts for sending sensitive work-related information, such as supporter details. Personal email accounts are not secure
- **Anyone could access or look at the information on her computer**
Get into the habit of locking your computer whenever you leave your desk
- **Anyone could read the documents if they are left lying around**
Never leave sensitive information lying around
- **Throwing sensitive documents in a waste bin is not a secure method of disposal**
Always keep sensitive information secure - even when you are disposing of it – use the confidential document bins

Information in the workplace

The impact of information loss

Jane manages a team of employees that devises surveys and collects public survey data. Take a look at how an unexpected data loss affected her most recent project:

"Last Friday one of my key team members left to take a job elsewhere. This created more of an impact than I could have imagined.

This particular employee had undertaken a complex survey on supporter feedback but, unfortunately, he had stored all the project information and results on the personal drive of his laptop. As is customary, the information on the computer was deleted when he left.

As a result, the information the team had researched and created is now lost permanently. This is a real blow to our current project."



Information in the workplace

The impact of information loss

So what are the immediate and potential consequences of this loss of information?



Business

"My biggest immediate worry is the overall financial cost and extra staff time needed for repeating the project. Losing information never looks good, and asking our supporters to repeat their feedback will also affect how they view the organisation."

Personal

"I was about to take some annual leave, but now I will need to cover the additional work of re-creating this information. I'm worried about being able to meet the project deadlines and the overall quality of the final report. This is going to affect my reputation within the organisation."



Confidential and sensitive information needs to be kept secure, with unauthorised access and modification prevented. However, it also needs to be available when required.

Information in the workplace

Opening the door to risk

Consider the following example. Jennie has left work in a hurry to go to a doctor's appointment. What has gone wrong?

Jennie is leaving the office in a hurry to get to a doctor's appointment. As she leaves, she sees a man heading into the office that she doesn't recognise. Instinctively she holds open the door for him assuming that he must be a member of staff.

Once Jennie has attended her appointment, she heads back to the office. Unfortunately, in her rush to leave early, she forgot to take her security pass with her.

As she is rummaging through her handbag, the receptionist buzzes her in. Jennie gratefully heads back to her desk.



Information in the workplace

Facing the consequences

What are the possible consequences of Jennie's actions?

➤ **Poor security could have exposed the organisation to risks**

By ignoring the security procedures and letting an unknown person into the office, Jennie and the receptionist are exposing the organisation and their colleagues to risks. Jennie should have challenged the stranger rather than hold the door open for him. The receptionist should have checked that Jennie was a member of staff before allowing her to enter the building

➤ **Personal safety for all employees could have been at risk**

In extreme cases there is a chance that a stranger who has gained access to the building could cause physical harm to employees or even pose a terrorist threat. Never put colleagues at risk. Make sure you remain vigilant, challenge the presence of strangers and never provide unauthorised access

➤ **Equipment or belongings could have been stolen**

It's possible that the stranger could have stolen office equipment or personal belongings. This could lead to a financial loss for the organisation and the affected individuals. Equipment can also store sensitive information that could find its way into the public domain

Information in the workplace

Summary

Let's recap the key points:

- Whatever your work environment, you are responsible for protecting information
- The workplace is full of potential risks - know where they are
- Dispose of information correctly
- Make security your priority
- Think about security and availability



A person wearing a dark purple sweater and blue jeans, carrying a yellow backpack, is standing on a train platform. They are holding a smartphone in both hands and looking at the screen. The background shows several parallel train tracks receding into the distance.

Working on the move

Working on the move

Working on the move works

What are the benefits of working on the move?

Working on the move can give you greater flexibility than working in an office environment.

This in turn can lead to a better work/life balance and increased flexibility with your personal life.

Working on the move means you can make better use of your time to make you more efficient and productive.

Technology means you can now keep in touch with your colleagues and contacts more easily when you are away from the office.



Working on the move

Think before you leave

Before you take information out of a secure environment, ask yourself these four questions:

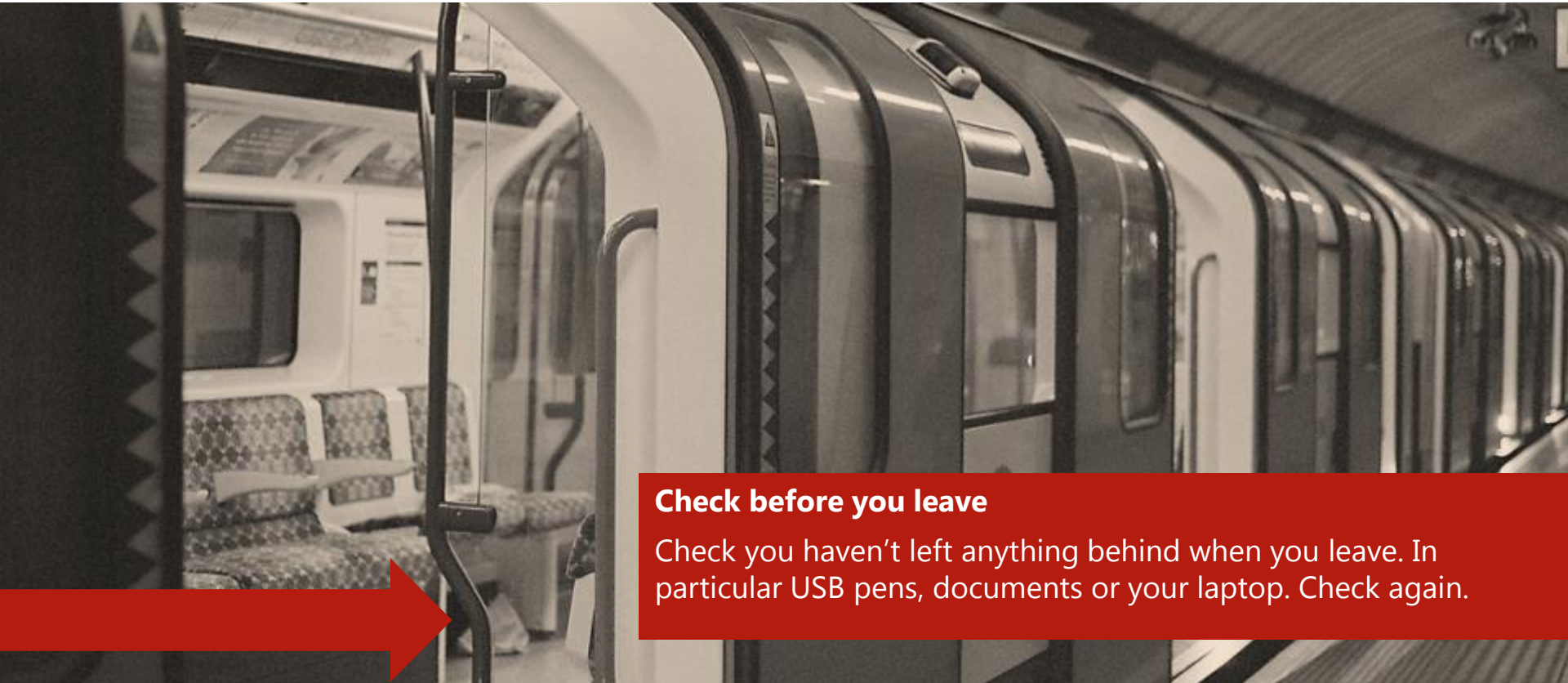
- What information am I taking?
- Am I allowed to take it?
- Am I familiar with my organisation's guidance on carrying information?
- Is it stored securely?



Working on the move

Different places mean different risks

When working outside of the traditional office space, information immediately becomes more vulnerable. So take extra care to avoid unnecessary risks.



Check before you leave

Check you haven't left anything behind when you leave. In particular USB pens, documents or your laptop. Check again.

Working on the move

Different places mean different risks

When working outside of the traditional office space, information immediately becomes more vulnerable. So take extra care to avoid unnecessary risks.



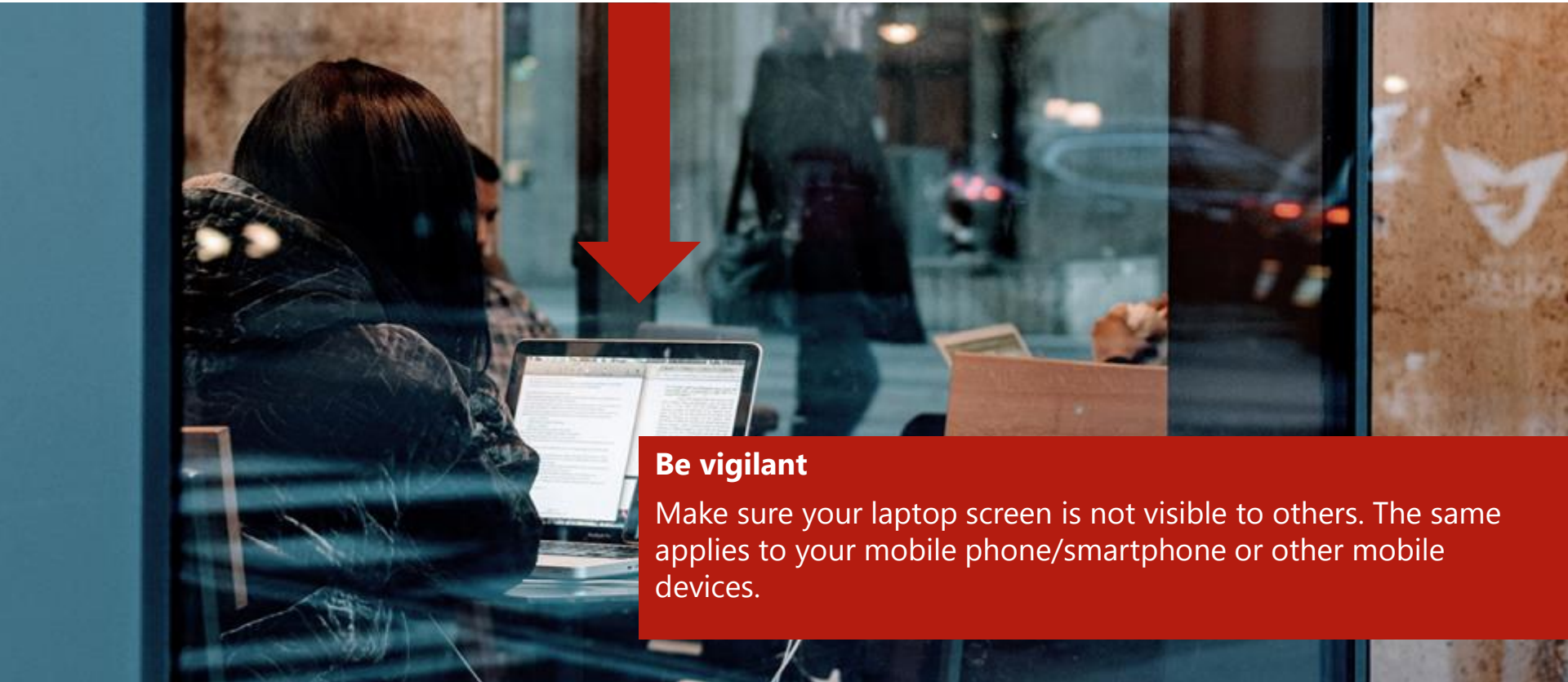
Work tidily

Work tidily and with care. Ensure no information is on display.

Working on the move

Different places mean different risks

When working outside of the traditional office space, information immediately becomes more vulnerable. So take extra care to avoid unnecessary risks.



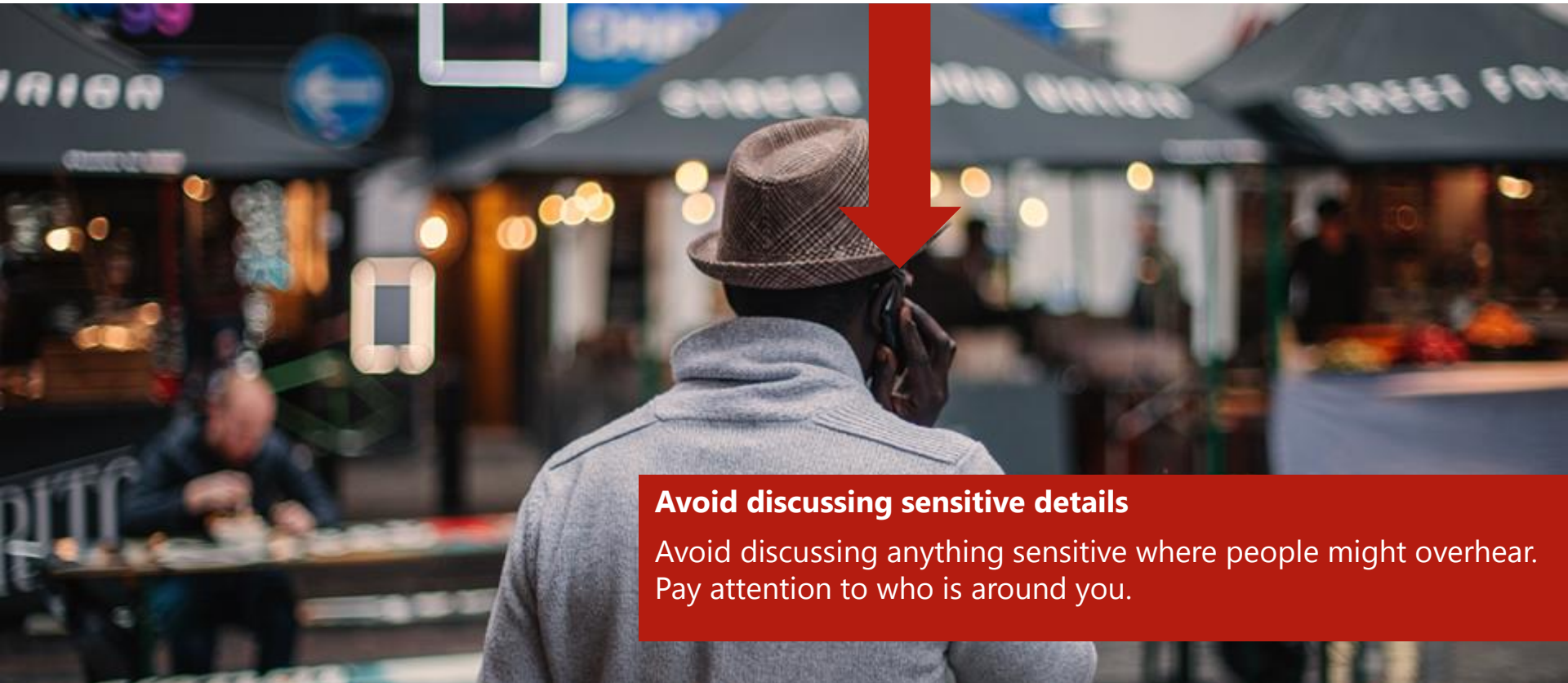
Be vigilant

Make sure your laptop screen is not visible to others. The same applies to your mobile phone/smartphone or other mobile devices.

Working on the move

Different places mean different risks

When working outside of the traditional office space, information immediately becomes more vulnerable. So take extra care to avoid unnecessary risks.



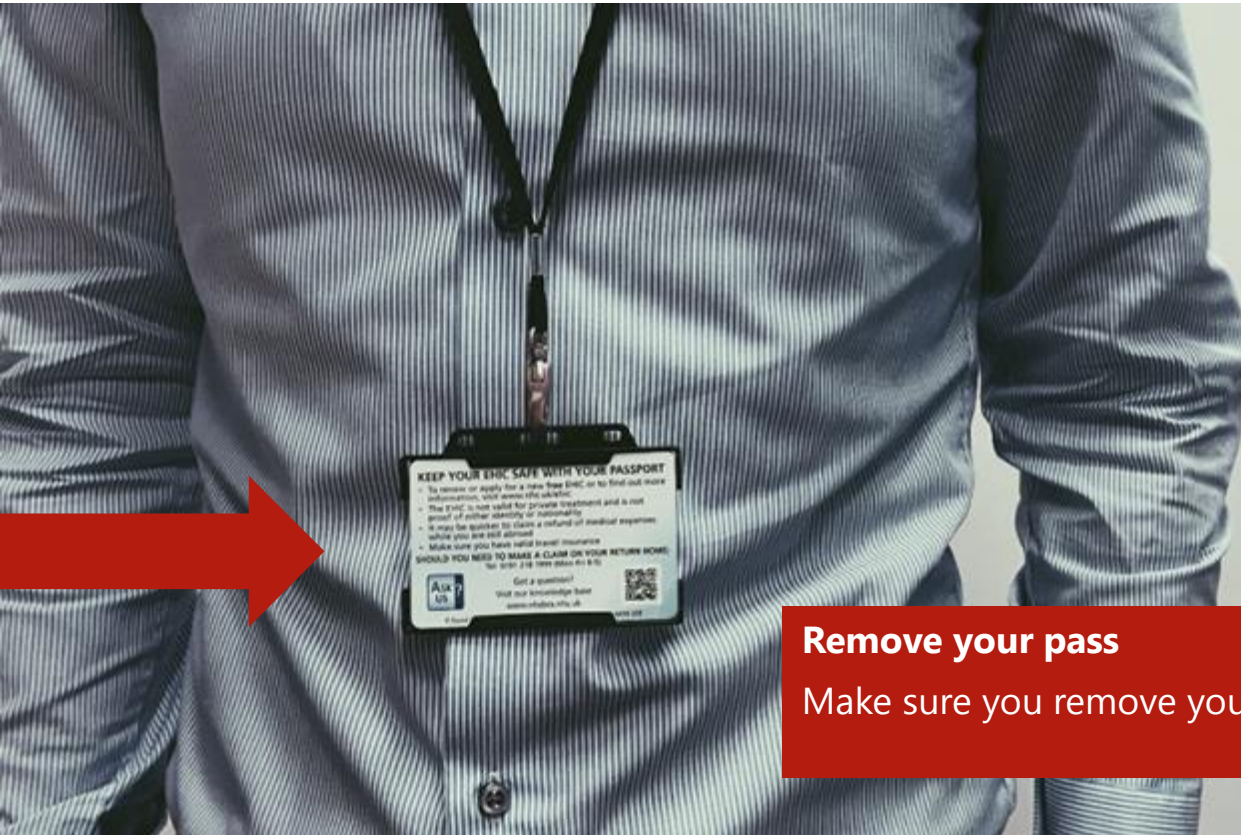
Avoid discussing sensitive details

Avoid discussing anything sensitive where people might overhear. Pay attention to who is around you.

Working on the move

Different places mean different risks

When working outside of the traditional office space, information immediately becomes more vulnerable. So take extra care to avoid unnecessary risks.



Remove your pass

Make sure you remove your pass when you leave work.

Working on the move

Disclosing sensitive information

Even work-related environments pose risks to information security. Consider this example:

Richard is attending a conference in London. It's lunchtime and he has just bumped into old colleagues. Richard starts discussing a new project he is working on - the development of a new product for the healthcare sector. He also starts discussing some of the medical data of patients.

The project is a new initiative for Richard. He has provided a lot of detail to his old colleagues and their company may be able to supply some of the components for the new product.



Working on the move

Disclosing sensitive information

Even work-related environments pose risks to information security. Consider this example:

Behind them, some other attendees are also eating. One of them works for a competitor and is very interested in the new product Richard is developing for his company. The private confidential patient information was also overheard.



Working on the move

The unfortunate consequences

As you can see below, Richard's lack of judgement has consequences:

➤ Legal

There could be legal consequences if the fairness of the supplier selection process is jeopardised. Also, discussing confidential patient information with unauthorised people is a breach of the Data Protection Act. Remember, once information becomes public, it becomes impossible to control


➤ Reputation

Richard has put both his own reputation and that of his organisation on the line. Remember, more than one reputation is at stake when confidential information is disclosed

➤ Commercial

By discussing commercially sensitive information openly, Richard has given an unfair advantage to a supplier. This could make it harder for his organisation to get the best deal possible

In CAFOD's context – think of sharing information about a possible fraud case in a project or programme while at a conference with colleagues from other INGOs and donors



Always report lost or missing information immediately to your manager. The consequences of trying to hide a loss can be far worse.

Working on the move

Working from home

You might feel that your own home is the most secure environment of all. However, you still need to consider the risks.

- **Document disposal:** Don't throw sensitive or confidential documents into the bin. Dispose of paper documents just as securely as you would in the office
- **Documents lying around:** Get into the habit of keeping information discreet. Don't just leave things lying around for others to see
- **Mobile phone:** When dealing with sensitive information over the phone, just be aware of who might overhear, purposely or not
- **Protecting information:** If possible, sensitive matters related to the organisation should not be conducted using personal laptops or home computers. A company laptop with all the necessary security controls should be used. If required, confidential and commercially sensitive documents should be password protected and the laptop hard drive encrypted. Also consider protecting USB pens, password protect documents, or use encrypted pens
- **Insecure networks:** Web-based email accounts are particularly risky. Avoid using personal email addresses to send confidential organisational information. Always check your organisation's policies. Connect to the business network using a Virtual Private Network (VPN). If using a wireless network ensure a minimum of Wi-Fi Protected Access 2 (WPA2) with a good security key

Working on the move

Summary

Let's recap the key points:

- Working on the move offers benefits and risks
- Consider the risks before you leave a secure environment
- Don't discuss sensitive information where you can be overheard
- Accidentally disclosing sensitive information can have serious operational, reputational, legal and financial consequences
- Report lost or missing information immediately
- Information needs to be protected when working from home





Staying safe online

Staying safe online

Things are not always as they seem

The internet is an amazing tool and increasingly important to our daily lives. Like any other field, however, it is not without risk. A growing number of criminals use it to commit cyber crime and to exploit others.



"I hack into private email accounts to obtain personal or business information. I'm particularly interested in obtaining a company's intellectual property to sell to other businesses or building fake profiles in order to steal a person's identity."



"I pretend to be someone else on Facebook. This may help me trick you into handing over sensitive company information. I may be a competitor or employed by a competitor to obtain information."

Staying safe online

Things are not always as they seem

The internet is an amazing tool and increasingly important to our daily lives. Like any other field, however, it is not without risk. A growing number of criminals use it to commit cyber crime and to exploit others.



"I send millions of spam emails designed to trick you into handing over money. I may also target particular individuals in your business (spear phishing) that may be of interest."



"I contract my services to foreign companies who wish to steal information from UK companies in order to gain a competitive advantage. I write malware that can be used to steal information from your business including intellectual property."

Staying safe online

Things are not always as they seem

The internet is an amazing tool and increasingly important to our daily lives. Like any other field, however, it is not without risk. A growing number of criminals use it to commit cyber crime and to exploit others.



"When I disagree with your business operations, products or services, I try to disrupt the operation of the business by attacking and shutting down your website."



"I used to smuggle drugs, now I make more money trading stolen credit card details on the internet."

Millions of spam emails are sent to organisational email addresses every month, online crime makes more money than the illegal drugs trade and online ID theft is the fastest growing ID crime. The overall cost to the UK economy from cyber crime is £27 billion per year.



Staying safe online

Email threats

Despite the security precautions taken by your organisation, emails can still pose a threat.

Your purchase is complete

Mervyn Operator <mervynreceiptgenerator@gmail.com>

Sent: Fri 27/01/2017 12:15

To:

Message image.jpg (2 MB)

Dear sir,

Please see your order confirmation.

Please view the attachment to confirm you are happy.

You can also access your order here:

www.mervynoperatorordering.co.uk

Kind regards,

customer team

The sender (From)

Look at the sender's email address. Ask yourself these questions:

- Do I know this person?
- Is this their usual email address?
- Be aware, spammers attempt to send email using your legitimate friends, colleagues or family email addresses. They may have obtained these email addresses from contact lists using malware installed on their computers

Staying safe online

Email threats

Despite the security precautions taken by your organisation, emails can still pose a threat.

Your purchase is complete

Mervyn Operator <mervynreceiptgenerator@gmail.com>

Sent: Fri 27/01/2017 12:15

To:

Message image.jpg (2 MB)

Dear sir,

Please see your order confirmation.

Please view the attachment to confirm you are happy.

You can also access your order here:

www.mervynoperatorordering.co.uk

Kind regards,

customer team

Subject

You should always give your emails meaningful subject lines, and expect to receive the same. Ask yourself these questions:

- Does this email subject look unusual? (for instance, it uses a zero instead of an O)
- Are there spelling mistakes?
- Is there excessive punctuation?

Out of the ordinary or poorly written subject lines may hint at a fraudulent or spam email.

Staying safe online

Email threats

Despite the security precautions taken by your organisation, emails can still pose a threat.

Your purchase is complete

Mervyn Operator <mervynreceiptgenerator@gmail.com>

Sent: Fri 27/01/2017 12:15

To:

 Message  image.jpg (2 MB)

Dear sir,

Please see your order confirmation.

Please view the attachment to confirm you are

You can also access your order here:

www.mervynoperatorordering.co.uk

Kind regards,

customer team

Links

Be wary of links in emails. Links can easily be disguised and may take you to malicious websites.

Staying safe online

A dangerous email

Spam, fraudulent and malware infected emails are sent every day, to both work and personal email addresses. Consider this example.

It's Friday morning and Colm logs on to his computer. He receives an email telling him that his inbox is full. The email asks him to click on the link to upgrade his mailbox.

Colm clicks the link and several browser windows open, none of which seem to be related to the link. He closes the windows but now his PC seems slower. He phones the IT helpdesk and goes to a meeting.

When Colm returns to work, most of the computers in his office are playing up, the phones are ringing and no one can log in. He overhears that a virus has seriously infected the network.



Staying safe online

Consequences and lessons

So what are the consequences of Colm's actions, and what lessons can you learn from his mistake?

➤ **A simple click**

By simply clicking on a link, Colm downloaded a piece of malware from the internet, which then spread across the network and infected the office computer systems

Remember: unexpected emails, particularly from unknown senders, should always be treated suspiciously.

➤ **Massive disruption**

The malware was difficult to remove and many staff were unable to work for several days, costing the organisation thousands of pounds to resolve and disrupting critical activities

Remember: if you are not sure about an email you have received, get in touch with your IT department to have it checked.

Staying safe online

Consequences and lessons

So what are the consequences of Colm's actions, and what lessons can you learn from his mistake?

➤ **Reputational damage**

The organisation was unable to maintain services to its supporters and partners for several days. This affected the reputation of the organisation.

Remember: if you suspect malware is attacking your computer, don't try to cover it up. Report it immediately to avoid any further damage.

➤ **Report it**

Colm was embarrassed by his mistake and mortified about the damage that had been caused

Remember: internet links within emails and documents can easily be marked or made to appear legitimate. Criminals often use this method to trick people into visiting websites where they can exploit them or unknowingly download malware.

Staying safe online

Top web tips

There are plenty of things you can do to avoid being caught out by threats on the internet.

Think carefully when entering personal or financial information over the internet. Try to make sure you are certain that the website is trustworthy. Look for a padlock and https within the website address. If possible, verify the site by validating the certificate. Click the padlock to check the site is legitimate. The website address should correspond to the name of the organisation on the certificate.



Staying safe online

Top web tips

There are plenty of things you can do to avoid being caught out by threats on the internet.

Use extra caution when using internet cafes, public Wi-Fi or shared computers. When you've finished, be sure to log out and take all your information with you. Avoid entering sensitive information when you are operating in these areas.



Staying safe online

Top web tips

There are plenty of things you can do to avoid being caught out by threats on the internet.

Use strong passwords (containing letters, upper and lower case, numbers and symbols), change them regularly and try not to use the same password for different accounts. This is the easiest way to help protect your information. Do not share your passwords with colleagues.



Staying safe online

Top web tips

There are plenty of things you can do to avoid being caught out by threats on the internet.

If you use a wireless router, check it is password protected. Ideally, the wireless router should be using a secure connection. When working remotely always connect to the office network using a secure connection, especially in public areas using wireless connectivity.

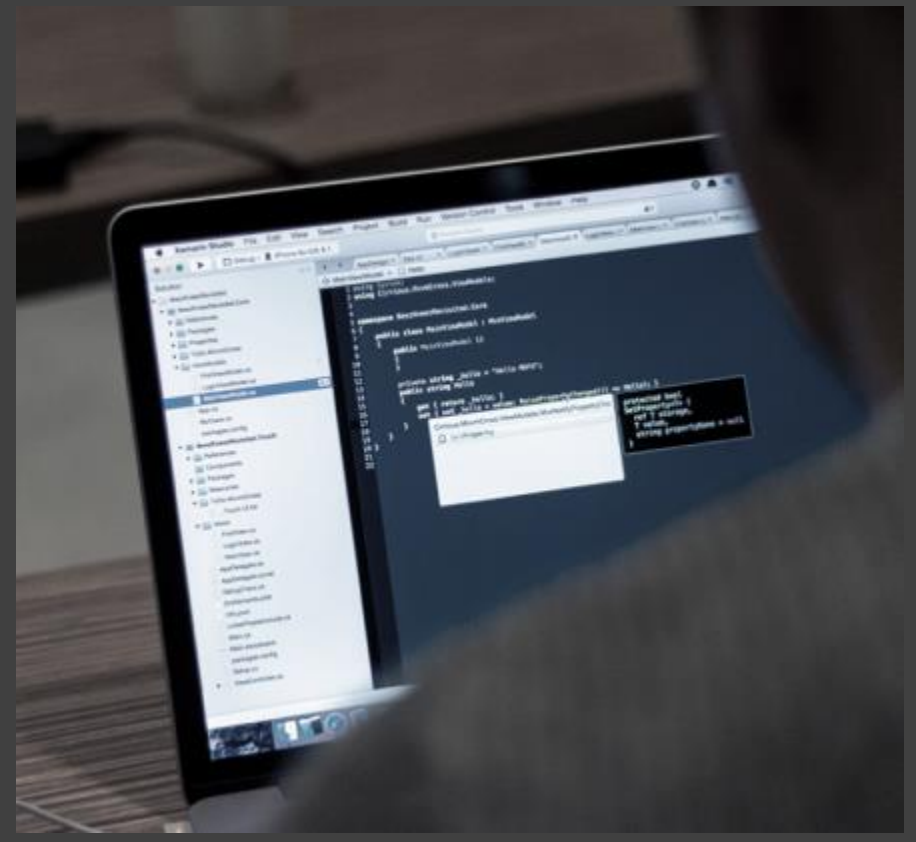


Staying safe online

Top web tips

There are plenty of things you can do to avoid being caught out by threats on the internet.

Be careful when clicking on internet banners and pop-ups, they could potentially download malware.



Staying safe online

Top web tips

There are plenty of things you can do to avoid being caught out by threats on the internet.

Be careful when clicking on links provided by search engines, you could be taken to an untrustworthy site.



Staying safe online

The pros and cons of social networking

Social networking is a great way to connect with people, share media and exchange information and ideas. But be aware of the risks.

➤ **The positive side of social networking:**

- You can make connections with communities of people with similar interests
- You can reconnect with old friends and meet new people
- You can share photos with your friends and family
- You can easily invite friends to meetings and parties
- You can share information and ideas

➤ **The potential risks of social networking:**

- Your personal information may be easily available to others
- You may expose sensitive organisational information
- You may lose control of your photos once they are on the internet
- Sites may be used to spread malware and malicious applications

Staying safe online

Social media offers positive benefits to organisations

Social media can be used to reach groups of people who do not respond through more traditional methods of communication. Take a look at these two examples of how social media can provide positive benefits.

Companies use cyber challenges and social networking to promote careers in cyber security. Some of the campaigns invite applicants to solve a visual code posted on a website, through advertisements on social networking sites, blogs and forums. Those who successfully crack the code are re-directed to the agency's recruitment website.



Staying safe online

Social media offers positive benefits to organisations

Social media can be used to reach groups of people who do not respond through more traditional methods of communication. Take a look at these two examples of how social media can provide positive benefits.

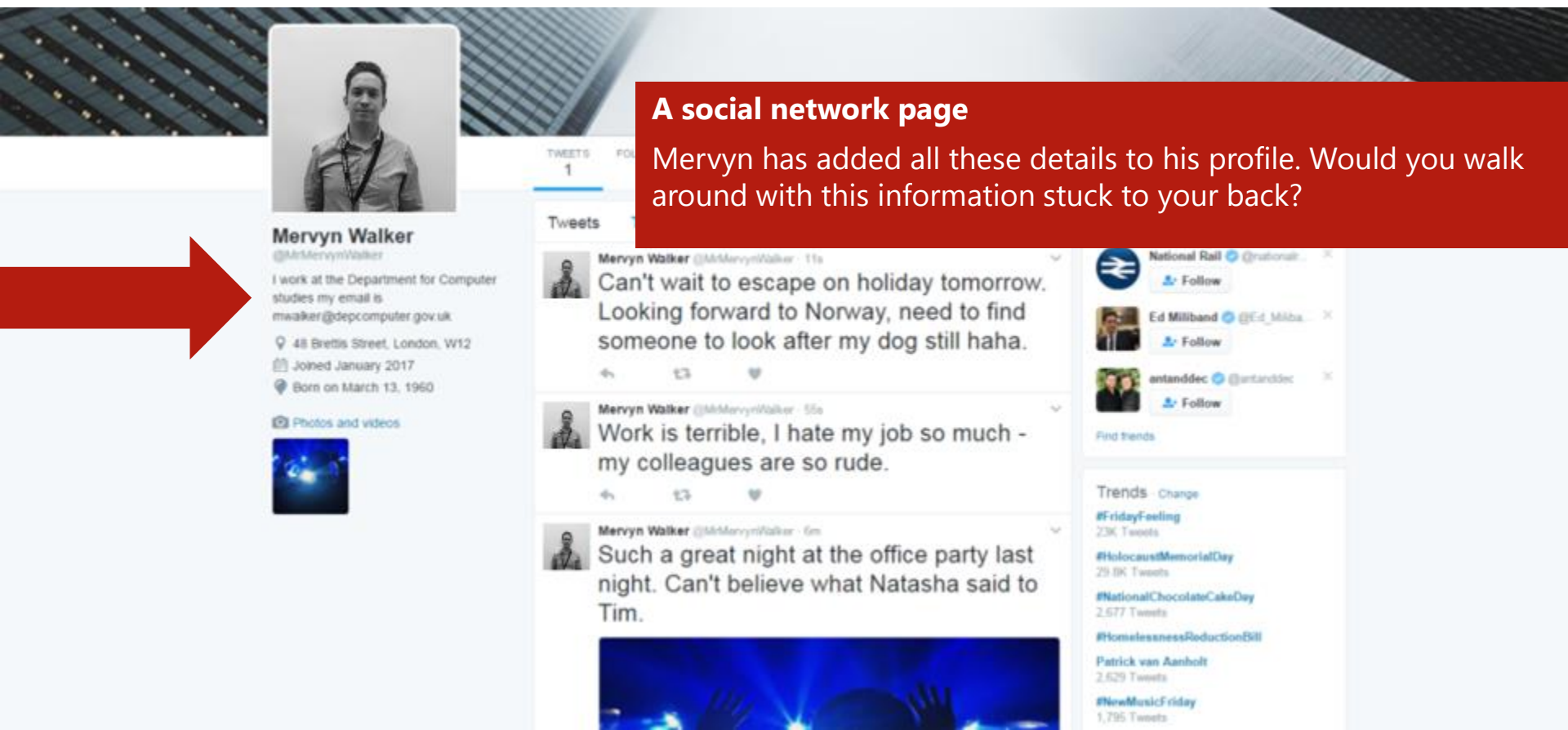
The Transport for London Live Traffic Camera feed provides still images from 177 CCTV cameras in key locations across the capital. People are able to select a location and view the CCTV images on Google Maps.

Google Maps provide images of, and information on, restaurants and other businesses. Images provide a location description, date and timestamp, and are refreshed at least every three minutes. This can help the public plan their route through London.



Staying safe online

Spot the risks



A social network page

Mervyn has added all these details to his profile. Would you walk around with this information stuck to your back?

Staying safe online

Spot the risks

On holiday

Mervyn mentioned that he's going on holiday for two weeks. This implies his house is going to be left empty.

Mervyn Walker
@MrMervynWalker
I work at the Department for Computer

Joined January 2017
Born on March 13, 1960

Photos and videos

Mervyn Walker @MrMervynWalker · 11s
Can't wait to escape on holiday tomorrow. Looking forward to Norway, need to find someone to look after my dog still haha.

Mervyn Walker @MrMervynWalker · 55s
Work is terrible, I hate my job so much - my colleagues are so rude.

Mervyn Walker @MrMervynWalker · 6m
Such a great night at the office party last night. Can't believe what Natasha said to Tim.

National Rail @nationalrail · Follow

Ed Miliband @Ed_Miliband · Follow

antanddec @antanddec · Follow

Find trends

Trends Change

- #FridayFeeling 23K Tweets
- #HolocaustMemorialDay 29.9K Tweets
- #NationalChocolateCakeDay 2,577 Tweets
- #HomelessnessReductionBill Patrick van Aanholt 2,529 Tweets
- #NewMusicFriday 1,795 Tweets

Staying safe online

Spot the risks



Mervyn Walker

@MrMervynWalker

I work at the Department for Computer studies my email is mwalker@depcomputer.gov.uk

48 Brettis Street, London, W12

Joined January 2017

Born on March 13, 1960

Conversations about work

It is not appropriate to discuss work issues on personal social networking sites, you can never be sure who will read the information and what they will use it for.

Tweets

Mervyn Walker @MrMervynWalker · 11s
 Can't wait to escape on holiday tomorrow. Looking forward to Norway, need to find someone to look after my dog still haha.

Mervyn Walker @MrMervynWalker · 55s
 Work is terrible, I hate my job so much - my colleagues are so rude.

Mervyn Walker @MrMervynWalker · 6m
 Such a great night at the office party last night. Can't believe what Natasha said to Tim.



Find trends

Trends Change

#FridayFeeling

23K Tweets

#HolocaustMemorialDay

29.9K Tweets

#NationalChocolateCakeDay

2,577 Tweets

#HomelessnessReductionBill

Patrick van Aanholt

2,529 Tweets

#NewMusicFriday

1,795 Tweets

Staying safe online

Spot the risks



Mervyn Walker

@MervynWalker

I work at the Department for Computer studies my email is mwalker@depcomputer.gov.uk

48 Brettis Street, London, W12

Joined January 2017

Born on March 13, 1960

Photos and videos



Public profile

This page is visible to the general public, not just Mervyn's friends and family. Make sure that you check your privacy settings regularly as they can change without warning.

TWEETS
1

Tweets



Mervyn Walker @MervynWalker · 11s

Can't wait to escape on holiday tomorrow. Looking forward to Norway, need to find someone to look after my dog still haha.



Mervyn Walker @MervynWalker · 55s

Work is terrible, I hate my job so much - my colleagues are so rude.



Mervyn Walker @MervynWalker · 6m

Such a great night at the office party last night. Can't believe what Natasha said to Tim.



National Rail @nationalrail

Follow



Ed Milliband @Ed_Miliban

Follow



antanddec @antanddec

Follow

Find trends

Trends Change

#FridayFeeling

23K Tweets

#HolocaustMemorialDay

29.9K Tweets

#NationalChocolateCakeDay

2,577 Tweets

#HomelessnessReductionBill

Patrick van Aanholt

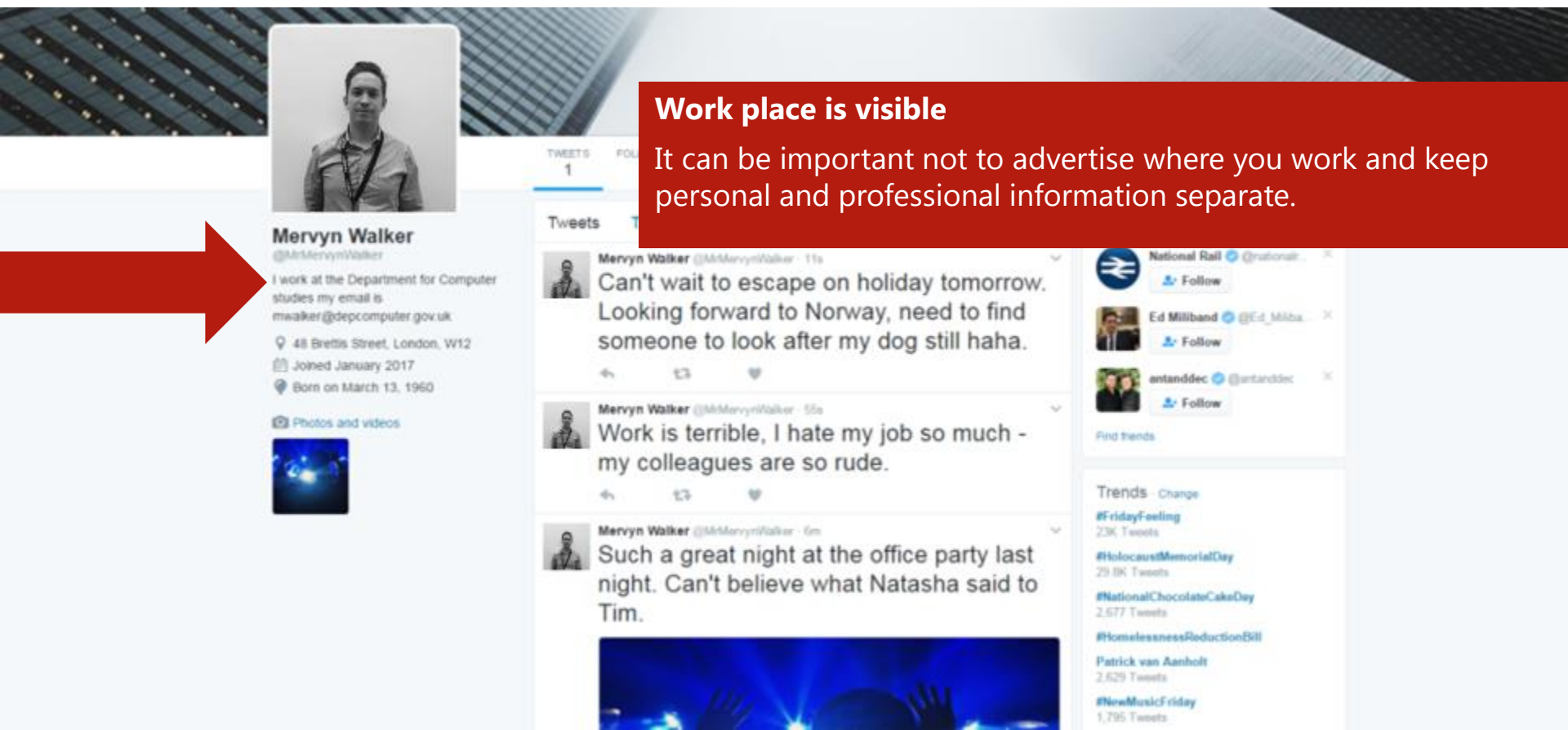
2,529 Tweets

#NewMusicFriday

1,795 Tweets

Staying safe online

Spot the risks



Work place is visible

It can be important not to advertise where you work and keep personal and professional information separate.

Staying safe online

Spot the risks



Mervyn Walker

@MrMervynWalker

I work at the Department for Computer studies my email is mwalker@depcomputer.gov.uk

48 Brettis Street, London, W12

Joined January 2017

Born on March 13, 1960

Photos and videos



Photos of an office party

Remember that photos uploaded to the internet are almost impossible to remove and can quickly spread out of your control.

TWEETS
1

Tweets

Mervyn Walker @MrMervynWalker · 11s
Can't wait to escape on holiday tomorrow. Looking forward to Norway, need to find someone to look after my dog still haha.

Mervyn Walker @MrMervynWalker · 55s
Work is terrible, I hate my job so much - my colleagues are so rude.

Mervyn Walker @MrMervynWalker · 6m
Such a great night at the office party last night. Can't believe what Natasha said to Tim.



National Rail @nationalrail Follow

Ed Miliband @Ed_Miliband Follow

antanddec @antanddec Follow

Find trends

Trends Change

#FridayFeeling 23K Tweets

#HolocaustMemorialDay 29.9K Tweets

#NationalChocolateCakeDay 2,577 Tweets

#HomelessnessReductionBill

Patrick van Aanholt 2,629 Tweets

#NewMusicFriday 1,795 Tweets



Staying safe online

A tweeting disaster

Although a tweet only has up to 140 characters, those few characters can still cause reputational damage to both individuals and organisations. Consider this example.

Jason is at his desk and is tweeting about his current project. Although the project is a high-profile organisational one, he is tweeting that: "nobody seems to know what they're doing round here".

One of Jason's friends finds this tweet amusing. He re-tweets and puts it in context. He has 3,000 followers so the message spreads quickly.

Jason deletes the tweet, but the information has spread and has already been picked up by the media. There is reputational damage to the organisation and Jason's position needs to be evaluated by his manager.



Staying safe online

The consequences

Don't underestimate the power of 140 characters.

As social networking continues to grow dramatically, the reach and influence continues to expand at an exponential rate.

The speed at which the internet virally spreads information means you **very quickly lose control** over anything you post.



Staying safe online


Summary

Let's recap the key points:

- The internet has a lot to offer, don't be afraid to use it
- As the internet gets more advanced, so does internet crime
- Email allows criminals an attack approach, so make sure you can spot the signs
- If you suspect malware, get in touch with your IT department immediately
- Minimise online risks by taking extra care, just as you would in real life
- Social networking is great, but consider the impact of posting information. Do not post confidential organisational data or personal sensitive information, such as your date of birth or home address
- Once information is on the internet, it is difficult to remove



Fraud



Fraud is a criminal activity where deception is used for personal gain or to cause a loss.

Fraud

Failure to disclose information

The Fraud Act (2006) describes three ways in which fraud can be committed. These are just a few completely fictitious examples to illustrate those three types of fraud.

False representation

"As a director of a partner I manipulated the financial accounts in order to record expenditure that was not actually made. This allowed me to divert some grant money for myself."

Accepting a bribe

"As an project officer I work with partners to review their reporting and accounting. I know that they are not paying all taxes due to the local tax authorities. But I keep quiet about it as they give generous gifts and accommodation for myself and my family."

Abuse of position

"As a senior manager I am often consulted on decisions regarding suppliers. Recently I blocked a procurement decision to appoint a new, more cost-effective supplier. The director of the existing supplier is an associate of mine - I didn't want to upset him, as I get a good deal on things I buy from him personally."

Fraud

Impacts of fraud

The UK Fraud Costs Measurement Committee estimated in 2016 that fraud costs UK organisations around £144 billion every year. The worldwide figure is unimaginable!

- Fraud can prevent an organisation from growing, employing new staff and maintaining a good reputation. In CAFOD's sector this impacts government attitudes to overseas aid and is likely to lead to every increasing and more burdensome compliance that will stretch our programme teams and partners to the limit.
- Fraud can cause financial impact, reputational damage and reduce morale in an organisation.
- Money obtained by individual fraudsters can be used to fund organised crime and other serious crime – a particular concern for CAFOD is aid diversion to support terrorism.

Fraud

Fraud triangle

Fraud always involves three factors: means, motive and opportunity.

The key to stopping fraud is to break the 'fraud triangle' by reducing the **opportunity** for fraud, by having good internal controls that are followed and by creating a culture in which fraud is not tolerated.

A person's **motive** is difficult to prevent, if for example an employee is in debt, they may have a motive to commit fraud. However, an organisation that encourages discussion of personnel matters could help mitigate this issue.


All personnel (at CAFOD and our partners) have the **means** to commit to fraud.




Fraud

Spot a fraudster


Fraudsters come in many guises: suppliers, customers, colleagues or hardened criminals. It is important that you remain vigilant and can spot the signs of fraudulent behaviour.



A colleague I manage claimed inflated expenses. I spotted it because I always scrutinise expense forms before sending them off and query them if necessary.



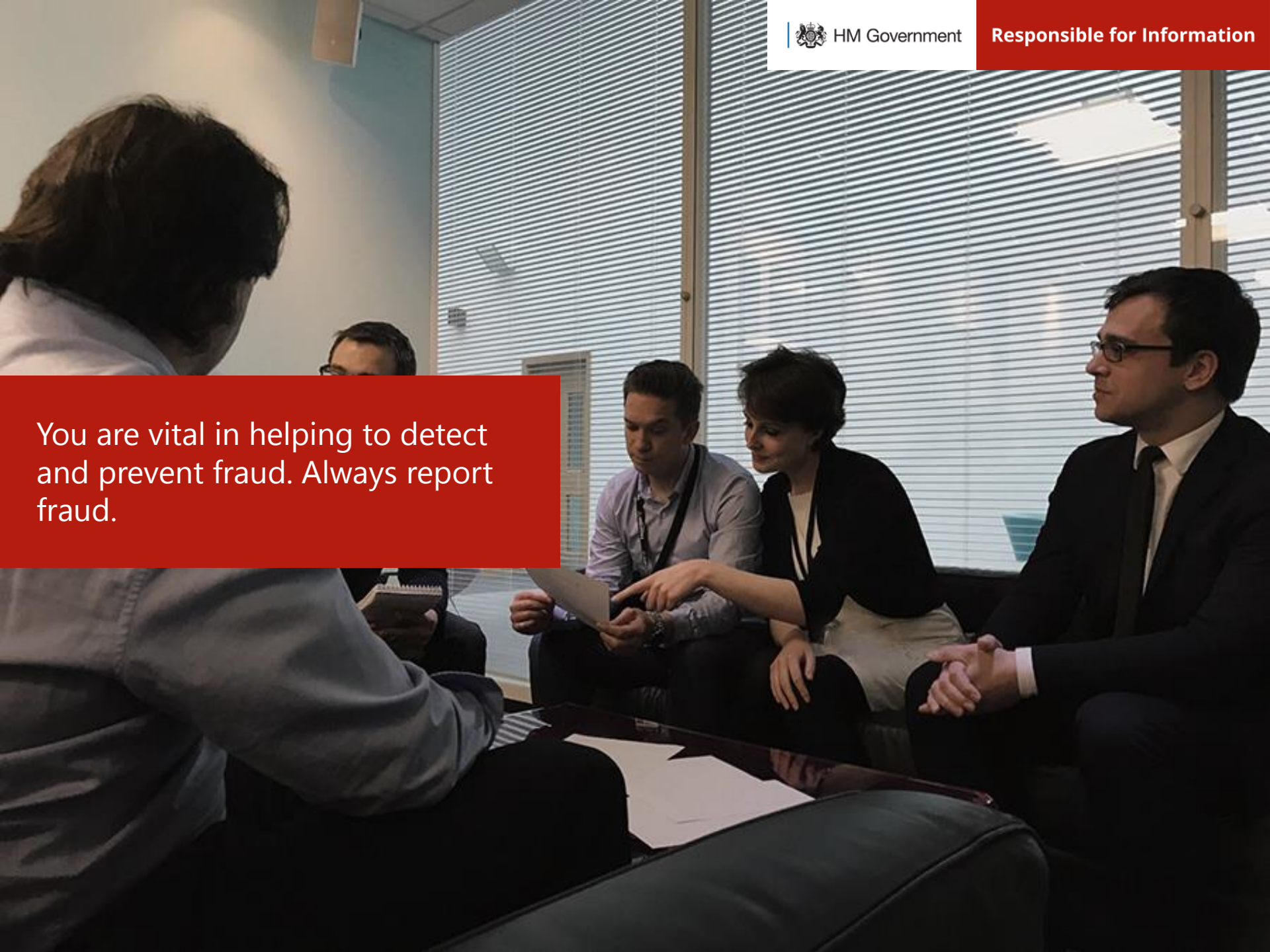
I spotted a fraudster when a contractor submitted a tender that was much lower than the other submissions. This made me suspicious.



I work as a finance manager and noticed one of our partners was providing copies of expenditure invoices that did not look real.



You are vital in helping to detect and prevent fraud. Always report fraud.



Fraud

What to do if you suspect fraud

➤ Do

- Act quickly
- Document the details
- Report it (using our Fraud Reporting procedures)
- Check our Fraud & Loss policy if unsure

➤ Do not

- Delay reporting
- Remove documentation
- Try to investigate it yourself
- Talk about it with colleagues or friends
- Approach or accuse individuals directly

Fraud

Bribery Act

The Bribery Act (2010) imposes heavy penalties on individuals found guilty of bribery offences, including both fines and imprisonment. You may be guilty of bribery whether or not you're aware that you have actually committed an offence. For more details, check our Anti-Bribery Policy.

Some sobering thoughts

"Bribery is estimated to raise the average Kenyan family's cost of living by 15%" *Transparency International 2011*

"83% of all deaths from building collapse in earthquakes over the past 30 years occurred in countries that are anomalously corrupt" *Nature Magazine, 12 January 2011*

Definition

"Bribery is the offering, giving, accepting or soliciting of any item of value or an advantage to another person to induce that person to improperly perform a relevant function or activity, or to reward them for improper performance."

Impact of Bribery

"Bribery and corruption are found in all countries. They hurt the poor disproportionately, diverting resources intended for development and humanitarian assistance and increasing the costs of basic public services. They undermine economic growth and are a barrier to poverty alleviation and good governance. Often, bribery and corruption can aggravate conflict and insecurity."

Bribery

CAFOD takes a zero tolerance approach to bribery in all forms including facilitation gifts, payments and favours. This includes overseas offices, partner organisations and agents. CAFOD does not tolerate bribery and does not accept the argument that in some circumstances there is no choice but to make facilitation payments or pay bribes either for operational efficiency or because of the humanitarian imperative.

Grant Agreements say

“The UK’s 2010 Bribery Act requires CAFOD to have in place effective measures for preventing bribery, where bribery includes the acceptance or payment of facilitation payments. Accordingly, no part of this CAFOD grant may be used for the payment of either bribes or facilitation payments.”

Accepting gifts

“In some countries, gift giving and hospitality are common. Genuine hospitality and the giving / receiving of gifts are not prohibited under the Bribery Act however it is important to note the CAFOD guidelines on anti-bribery when giving or receiving gifts or hospitality.”

Payment under Duress

“In all cases, the security and safety of staff, partners and representatives must not be compromised. Although CAFOD security procedures should minimise the likelihood, in some cases a payment under duress may need to be made. “Duress” includes a threat to safety and security and does not include the threat of delay or inconvenience.

A payment under duress is considered to be extortion and not bribery and should be reported as a security incident under CAFOD’s security procedure.”

Fraud

Summary

Let's recap the key points:

- Fraud is a criminal offence
- Fraud can be committed by anyone
- Report fraud immediately
- Fraud damages our ability to deliver our mission
- Fraud can seriously damage CAFOD's reputational if not handled appropriately
- We all have a role to play in preventing and detecting fraud
- Pay particular attention to our Anti Bribery policy



OGIL All content is available under the Open Government Licence v3.0

© Crown copyright, 2017