Ministry of Justice

Your guide to being security aware

Introduction to Security

This booklet is for Ministry of Justice people and contractors.

Being a government worker for a Department which handles large amounts of data on behalf of vulnerable people, means you need to be aware of how to manage the security risks involved in your job, how to keep yourself safe around government buildings and online, and what to do if there is a problem.

We have lots of measures in place to protect our staff, and our information, but it's you - our people - who can make the biggest difference.

Thank you for doing your part.

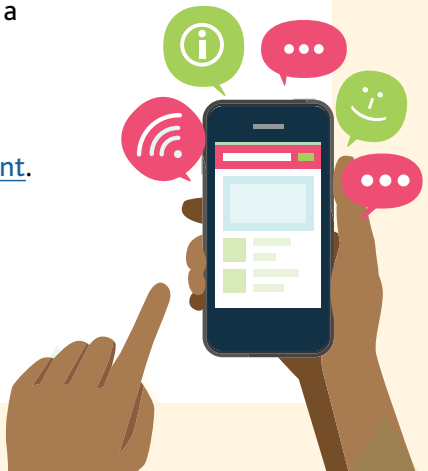
Online Safety

Every time you go online or someone posts information about you (e.g. Instagram) tracks are left behind - known as your Digital Footprint.

Photo sharing, dating apps, banking, shopping, gaming, professional and social networking all add to your footprint. We all need to be mindful of what we're sharing and what can be found out about us.

Here are some tips for staying safe online:

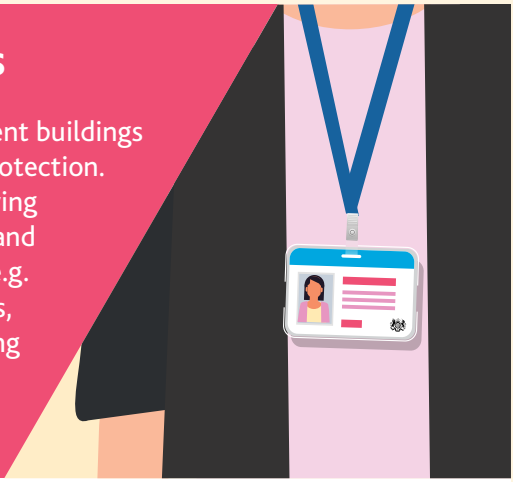
- Think carefully about what you post - and follow MoJ's social media policy.
- Review your social media settings regularly to ensure you aren't sharing too much.
- Don't share information that could make you a target (e.g. security clearance or ability to approve contracts).
- Review the advice in 'My Digital Footprint' booklet - www.cpni.gov.uk/my-digital-footprint.
- Enable multi-factor authentication on your personal social media and email accounts.



See intranet: Social media

Buildings and passes

Entrances and exits to government buildings are the first and last points of protection. You can play your part by following building pass security guidance and reporting any unusual activity (e.g. people loitering around buildings, unattended bags) to your building security team.



Tips on building and pass security:

- Always wear your security pass in the workplace, and remove it when you leave - it identifies you as a government worker.
- Challenge anyone who isn't clearly displaying a security pass on site.
- Report the loss or misuse of a pass to your building security team immediately.
- Ensure your security pass and keys are returned when you are moving jobs, taking a break, or leaving us.

See intranet: Building Security Pass

Information Security

As a department, we have been entrusted with large amounts of sensitive personal data on vulnerable individuals. Small actions can have big consequences, and we have a responsibility to keep personal data as safe and secure as we can.

How to keep information secure:

Immediately report any lost items, like laptops, phones or papers (see back page).

Lock your screen every time you leave your devices.

Choose a strong password (see intranet) and never share it with anyone.

Ensure you understand the sensitivity of your information and that you are handling and protecting it correctly (see Protecting Information on intranet).

Keep discussions about sensitive subjects to meeting rooms, not public areas.

Be aware who can see your screen if you're in a shared office or working remotely (e.g. cafes, trains, home). You can order a privacy screen from the IT catalogue.

Be mindful that you can be overheard by third parties in shared workspaces and public areas.

Be conscious of what you are saying on the phone outside the office.

See intranet: Information Security

Joiners, movers, leavers

If you have just joined the Department, are changing roles or teams, taking some time out (maternity leave, secondments etc), or leaving us, there are certain security procedures to be followed. Full procedures can be found on the HR pages of the intranet. The main things to remember are:

New staff - complete the corporate induction training and Civil Service Learning's 'Responsible for Information' training in your first week. Line managers should ensure new staff do these.

Movers / Leavers - if you are moving, leaving, or taking a break, you need to hand back your building pass, keys and devices. Line managers must complete the Leaver's Checklist, (see intranet).

See intranet: Induction, End or Change Employment

What to do if things go wrong

In the unlikely event that you're involved in a security incident, or if you lose a laptop or click on a suspicious email link – please report it immediately:

HQ:

If you have an IT incident (e.g. lose a device, click on a suspicious email link), please report it immediately here: Lost devices or other IT security incidents.

If you're involved in, or witness a security incident, or experience a data breach, please send a security incident report form (on the intranet) to: security@justice.gov.uk. If the incident happens outside of normal working hours, please call 0203 334 0324.

Please report things as quickly as possible - even if you're not completely sure of the details.

See intranet: Report an Incident or Breach

Executive Agencies and Arm's Length Bodies:

Executive Agency and Arm's Length Body (ALB) people should follow the reporting guidance on their local intranet.

And finally...

By taking these steps you can keep yourself, your colleagues and your organisation safe and sound. Thank you.

Further information:

Please contact the MoJ Security and Privacy team:
Email: security@justice.gov.uk
https://intranet.justice.gov.uk/guidance/security