Practical action to reduce the risk of privacy breaches

The following actions can help reduce the risk of a privacy breach occurring.

Privacy away from the work environment

Only collect, use or share information for professional purposes

- Only discuss issues outside your work environment that are publicly reported in the media (and don't disclose unpublished details).
- Don't share any information that could identify learners or their families outside of your work environment.
- Understand any obligations to keep information confidential and the extent of those obligations.

Keep information secure when not at work

- Do not take physical files or documents containing personal information out of your work environment unless absolutely necessary (e.g. taking learner assessment documents home for marking).
- Don't use portable electronic devices (e.g. USB sticks) to transfer work files
- Keep laptops secure, including in your car or at your home.
- Be mindful of other people who may see or hear personal information when working from home.
- Report any loss of information immediately.
- Conduct work meetings in private spaces.
- Only use secure password protected internet connection and use multi-factor authentication were available.

- Don’t work in public places or on public transport if there is a risk that other people can see your work or hear your conversations.

Privacy in the work environment

Keep people and information safe

- Have accessible acceptable use policies for devices and software products.
- Assess software products (e.g. apps, online tools) for privacy risks before you use them (e.g. complete a privacy impact assessment).
- Only give access to people who have a legitimate work purpose.
- Only provide people access to information if they have a legitimate purpose.
- Keep documents containing personal and sensitive information in secured cabinets.
- Use secure destruction bins for shredding any documents that contain personal information.
- Don’t recycle paper that has printed personal or sensitive information.
- Do not admit visitors into office or workspaces (including classrooms) without first checking who they are and if they should be there:
  - ask visitors to sign in
  - meet with visitor in areas where personal information is not visible.

- Look after your access card and report any loss immediately.
- Keep keys and any electronic access cards secure.
- Don’t provide your access card (if you have one) to other people.

Privacy at your workstation

Follow your organisation's IT, device use and cybersecurity policies

- Use strong unique passwords and change them when prompted.
- Don't write your passwords down or store them in locations that other people can access.
- Use two factor authentication where required.
- Ensure others can't see personal or confidential work or access your computer:
  - use your keyboard shortcut to lock your screen anytime you step away from your device
  - use 'secure print' when using the printer (if this is an option).
- Don't download or forward information personal emails, unauthorised devices or USB sticks – including your personal computer/laptop.
- Don't use unauthorised third-party applications or programmes on your work systems.
- Be vigilant of potential phishing and ransomware attacks – check before you click on anything and if in any doubt, don't click on links.
- Always restart your workstation/laptop when you've finished working on it for the day.

Access only what you need to

- Only access personal information if it's relevant to your work.
- Don't look up information for someone or about someone you know personally.
- Declare any perceived or actual conflicts of interest.

Ensure e-mail accuracy

- Pause and check your email content and recipients before you hit send.
- Use delay send (at least 2 mins) if it is available – if you need to retrieve an email in that time, go to your outbox.

- Check if you should be using bcc rather than cc when sending emails to a large number of recipients.

Share documents securely

- Where possible use a secure cloud sharing platform to share documents and attachments e.g. SharePoint, Google Workspace.
- Send attachments as pdf versions to prevent the receiver being able to modify or track changes made to the document.
- Use security features such as password protect when sending sensitive information – send the password separately via a different mechanism e.g. text, work online messaging platform (MS Teams or Zoom) or phone call.
- Check all attachments and email threads to ensure all content is suitable to share.
- Take extra care with spreadsheets:
  - do not send any spreadsheet containing sensitive or personal information
  - use security features such as password protect
  - check for hidden information behind tabs, rows and columns, filters and in pivot tables
  - consider whether a PDF copy of the information is more suitable than a spreadsheet.

Report any breaches or near misses

- Be aware your organisation's privacy breach management plan.
- Know what to do if you discover, or are informed about, a privacy breach or a near miss.
- Know the process for reporting privacy related incidents.
- Report all privacy related incidents.