[SLIDE 3]

The 'Security' Principle

It states that personal data shall be:

"..processed in a manner that ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

The key phrase here is, "appropriate technical and organisational measures". Data controllers are responsible for identifying what measures they need to have in place to keep personal data secure and the level of security that needs to be applied.

Having technical measures in place could help to protect systems from unauthorised access either internally or from an attack. They could also help to protect against any permanent loss of data and can ensure that the most up to date software protection is added.

It's important to remember, it is not just technical measures that will need to be looked at when securing personal data. Organisational measures, such as training and staff awareness are just as important. Controllers should consider what guidance is provided to staff and that this is regularly backed up with reminders and training updates. Many breaches come down to human error, so it is important to keep everyone's knowledge up to date.

SLIDE 4

So we will now have a look at some measures we would expect organisation to have in place.

Ask trainees if they can think of any measures an organisation could implement to prevent a data breach from occurring in the first place?

Here are some technical measures organisations should consider implementing:

Secure Wi-Fi - Allowing untrusted devices to connect to your network or using work devices on untrusted networks outside your office can put personal data at risk.

Access controls – Consider who can access what information and limiting this access where possible. Having different levels of permissions to access information can help protect against unauthorised access or data being visible.

Password protection - Change default passwords and limit the number of failed login attempts. They should consider Multifactor authentication. Effective authentication and authorisation can make the login process more resistant to phishing. These include two-factor authentication/multi-factor authentication, password managers, and alternative login mechanisms such as biometrics

Firewalls - As your first line of defence, a well configured firewall can stop breaches happening before they get deep into your network.
Malware protection - You should have up to date anti-virus or anti-malware products regularly scanning your network to prevent or detect threats.

Data back-up - Backups should not be permanently visible to the rest of the network and at least one of your backups should be off site. Don't leave backup drives unattended and lock them away when not in use. Also, make sure you know what data is being stored in the cloud.

Encryption - Ensure that data can only be accessed by authorised users by encrypting it.

SLIDE 5

Some measures that organisations can implement to prevent a breach from occurring in future include:

Security Policies and Procedures: They should have a security policy, including for agile workers and electronic devices. For example, some electronic devices let you remotely disable or wipe them. Staff should be reminded when working in public spaces to use secure networks, be aware of their surrounding and who can see the information. If organisations have a shop, office, or other premises, visitors shouldn't be able to wander unaccompanied in areas normally restricted to staff.

Organisations should ensure that any policies and agreements in place with staff cover their requirements when handling personal data on behalf of the organisations. These agreements should emphasise the importance of confidentiality and make clear what staff can and cannot do with the personal data they handle. For example, that data should not be accessed or shared with individuals without authorisations or a business need.

Confidential disposal of personal data: Over time, organisations may have collected large amounts of personal data. They should decide if they still need the data and if they do, make sure it's stored in the right place. E.g. If archived, they should ensure it's stored in a secure location. If they have data they no longer need, it should be deleted or destroyed in line with their data retention and disposal policies. If they use a contractor to

erase data or recycle the IT equipment, they should ensure they do it adequately or the controller may be responsible if personal data gathered by them is extracted from the IT equipment when it's resold.

Educate yourself and train your staff: Employees at all levels need to be aware of what their roles and responsibilities are. Organisations should ensure that staff are adequately trained and that they provide regular refresher training so that staff are aware of the correct processes to follow in order to prevent data breaches, or recognise threats such as phishing emails. Organisations should have an acceptable-use policy and training materials for staff, tailored to their roles.

An organisation should note that any technical measures in place (such as password protection) are only effective alongside the guidance provided to staff. It is no good having all the technical security in place if staff are not aware on how to set permissions or securely password protect documents.