Bring Your Own Device Policy (BYOD)

Introduction
Construction & Plant Assessments (CPA) recognises the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at home, at work or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. It is committed to supporting staff in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing CPA provided services on BYOD.

The use of such devices to create and process CPA information and data creates issues that need to be addressed, particularly in the area of information security.

CPA must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.

Information Security Policies
All relevant CPA policies still apply to staff using BYOD. Staff should note, in particular, CPA Information Security related policies. Several of these are directly relevant to staff adopting BYOD.

- Data Protection Policy
- Prevent Policy and Risk Assessments
- Social Media Policy
- E-Safety Policy

The Responsibilities of Staff Members
Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of CPA information (as well as their own information)
- Invoke the relevant security features
- Maintain the device themselves ensuring it is regularly patched and upgraded
- Ensure that the device is not used for any purpose that would be at odds with the CPA Data Protection Policy.

While CPA staff will always endeavour to assist colleagues wherever possible, CPA cannot take responsibility for supporting devices it does not provide.

Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data
- Keep information confidential where appropriate
- Maintain the integrity of data and information, including that on CPA premises
- Take responsibility for any software they download onto their device

Staff using BYOD must:

- Set up passwords, passcodes, or passkeys. These must be of sufficient length and complexity for the particular type of device.
- Set up remote wipe facilities if available and implement a remote wipe if they lose the device.
- Not hold any information that is sensitive, personal, confidential or of commercial value on personally owned devices. Instead they should use their device to make use of the many services that CPA offers allowing access to information on CPA services securely over the internet.
- Where it is essential that information belonging to CPA is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails.
- Ensure that relevant information is copied back onto CPA systems and manage any potential data integrity issues with existing information.
- Report the loss of any device containing CPA data (including email) to the Director.
- Be aware of any Data Protection issues and ensure personal data is handled appropriately.
- Report any security breach immediately to the Director.
- Ensure that no CPA information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party

Monitoring and Access

CPA will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks or both.
- Prevent access to a particular system.
- Take all necessary and appropriate steps to retrieve information owned by CPA.

Data Protection and BYOD

CPA must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 1998. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

CPA complies with guidance from the Information Commissioner's Office on BYOD they recognise that there are inherent risks in using personal devices to hold personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data.
CPA is registered with the ICO: Registration Number: Z3244453

Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the CPA facilities being withdrawn, or even a criminal prosecution.

Information to Help Staff

Any member of staff wishing to remotely access information saved by CPA, will have to gain permission from the director and gain a user name and password, which must be kept safe at all time, this again will be in conjunction with the polices named in section 2.

BYOD will normally be limited to the CPA Wi-Fi Network.