BRING YOUR OWN DEVICES CHECKLIST

What Happens Currently? • Do any employees use their own devices for business use and to store business data e.g. smartphones, tablets, laptops? • Analyse usage by department to get an overall picture of usage	
What Should Happen? • Are employees authorised for this use? If not has this been communicated to employees in a clear written format? • If employees are not allowed to use their personal devices for work this should be notified to them along with notice that any such use could be a breach of the company IT and email usage policy and could lead to disciplinary action up to and including dismissal. • If employees are authorised – a BYOD policy must be put in place and this should be discussed with the IT department in advance, so that any risks to Company data can be addressed.	
What Should Employees Know? • If employees are allowed to use their own devices ensure that your organisation has a BYOD policy in place and that it is communicated to employees regularly – at induction and at least once a year and any time it is amended or reviewed • The policy should contain clear instructions so employees understand that type of data can be stored on their personal devices and what data cannot and should not be stored on the device • Are there specific apps that the employee should not download to their personal device as it may pose a risk to business data stored on the device?? This should be discussed with IT and included in the policy. This should be assessed regularly for new apps that should be included	

Policies
• Ensure all policies are consistent – this may mean reviewing:
  ○ IT and Email Communications/Acceptable Usage Policies
  ○ Data Protection Policies
  ○ Confidentiality Policies
  ○ Bullying & Harassment Policies
  ○ Contract of Employment	

Confidential Company Information
• Confidential Company Information and client data BYOD policies should include the following:
  ○ A clear definition of the types of information that may be contained on devices which will be considered confidential business information
  ○ The protocol to be followed in the event that the device is lost or stolen e.g. IT to be contacted immediately to remotely wipe the device
  ○ The name of the relevant Data Protection Officer within the organisation. If your organisation manages personal data any loss/theft of the device may need to be reported to the Data Protection Commissioner	

Sensitive Information • Extremely sensitive confidential business information should only be able to be accessed by authorised individuals with special permissions on fully secured devices. This should be managed	

by IT and set out clearly in the policy. This information may require additional security so that it cannot be accessed from personal devices.	

Employee Data
• BYOD policies should include the following:
  ○ Notice to the employee that because of the BYOD policy there is potential that their own personal data may be stored/processed on a personal device and accessed by the business
  ○ The steps that will be taken by the organisation to ensure that any personal data contained on a personal device is kept secure
  ○ How the organisation will avoid accessing any other personal data belonging to the employee if it needs to access the device	

Security • Appropriate professional advice should be taken on the security software to be included on employees' personal devices • Once the relevant security software is installed employees should receive appropriate training on how to use the software to ensure the correct security measures are maintained • Have employees been briefed on using a strong password for their devices? • Have employee been briefed on what makes a password more secure? • Are employees reminded regularly to change their passwords? • Have employees been instructed to ensure that access to their device is locked or automatically locks after a short time? • Should employees install device locators on their devices so that they can located/wiped in the event of theft/loss e.g. Find my Iphone App	

Employee Monitoring
• The BYOD policy should include the following:
  ○ Clear directions on what information on a personal device may be monitored by the organisation
  ○ The reasons that any monitoring may be carried out by the business and the benefits any monitoring brings to the business
  ○ That monitoring will be restricted to times of business only to ensure it is proportionate	

Leaving Employment • BYOD policies should deal with what happens a device if the employee leaves employment • If the employer has subsidised the device it may be worthwhile considering purchasing the device from the employee so the organisation retains it • The policy should state that the employee must provide the device to the IT department to be cleansed of confidential company information before leaving employment • The policy should state that the employee must also sign a confirmation on leaving employment that they have not copied any confidential information onto their personal devices	