

Terms and Conditions for Departmental Devices

Permitted Use

1. I acknowledge that the Department permits me to use a departmental device (**Device**) for Departmental business on the following terms and conditions.
2. I acknowledge that in these terms and conditions:
 - a. **Departmental Information** means all and any part of Departmental intellectual property, information and data which has been or is created, acquired, collected, developed, modified, or stored at any time by, on behalf of, or for, the Department.
 - b. A reference to **access to** or **accessing** information includes creating, viewing, collecting, downloading, modifying, storing, processing, and transferring, the whole or any part of the information that is accessed.
3. I agree to only access information appropriate for the information security rating of the Device as defined in Appendix 4 of the *Mobile Communications and Portable Storage Device Policy* i.e. Corporate Standard/Corporate Confidential.
4. I will not use the Device to upload, store or transfer non-Departmental Information to, or on, the Department's databases, networks, hardware, and systems, including TRIM and the network file shares.
5. I will not delete any logs (for example, call history, SMS, iMessage) on the Device that are associated with actions undertaken which may be used for investigation purposes. I acknowledge that some non-Departmental Information may be accessed in the event of a security incident investigation as event logs, messages (for example, SMS, IM) pertaining to Departmental business may be in the same area as non-Departmental Information.
6. I agree to comply with all Departmental policies, including:
 - a. the *Acceptable Use of the Department's Technology Policy*;
 - b. the *Mobile Communications and Portable Storage Device Policy*; and
 - c. the *Password Policy*.
7. I acknowledge that I have Occupational Health and Safety responsibilities, and special care should be taken when using the Device. Refer to the '*OHS Guidelines for the use of Smart Phones and Tablets*' on the intranet.
8. I agree that the device should be used only to create and transport departmental records in the short term and these records must be transferred to corporate record keeping systems as soon as practical and then removed from the device. All electronic information that is updated and relates to department records must be stored securely on the network on a relevant database or system in accordance with the department's Records Management Policy.

Staff member initial here
Page one of three

Software, Back up and storage

9. I acknowledge that there will be software tool and security controls on the Device that protect the Department and Departmental Information, and I agree not to change configuration settings on the Device, including the lock screen.
10. I agree to use only Departmentally-managed technology or Departmentally-approved third-party storage solutions (for example, Cloud technology) to store Departmental information and records.
11. If the Device is an Apple-based iOS device, then by signing these terms and conditions, I also:
 - a. agree that I accept Apple's Terms and Conditions related to the corporate iTunes account;
 - b. agree that I will not change the Department's Apple account parameters which include the Department's ID, email address, and password, and that I will inform and assist the Department's Information Management and Technology workspace support team if I become aware that the account parameters have been changed on or via the Device;
 - c. agree that I will only use the corporate iTunes account with departmental iOS devices provided to me, and I will not use the corporate iTunes account for any personally-owned devices;
 - d. acknowledge that the IM&T Workspace support team will receive notifications of app purchases using the corporate iTunes account; and
 - e. acknowledge that if I update the Apple iOS ahead of being informed by Departmental IT staff that it is safe to do so, this may result in incompatibilities with the Department's environment and certain features of the Device.

Inspection, support and maintenance

12. I agree that the Department may inspect the Device for any purpose, and I will assist the Department to inspect the Device, immediately upon request by the Department.
13. I acknowledge that, in providing support and maintenance and during inspections, the Department may obtain access to non-Departmental Information on the Device, and I consent to the Department accessing such information.

Protection of the Department's interests

14. I agree to take any necessary steps to protect the Device and any Departmental Information contained within, or accessible via, the Device, including by:
 - a. complying with Departmental training and instructions;
 - b. protecting the Device from physical harm or damage;
 - c. not providing access to the Device to any unauthorised persons, including my family members;
 - d. safeguarding my credentials (including my password) by not sharing them with anyone, and by not storing them with the Device;
 - e. being aware of my surroundings when using the Device so Departmental business is not disclosed. This includes ensuring my screen is not viewed and my conversations are not overheard; and
 - f. storing the Device securely when I am not using it, including by keeping it out of common sight.
15. I agree that if the Department considers that the Device poses a threat to the Department's network or hardware, then the Department may disconnect the Device from the network or hardware without any prior notice to me.
16. I agree that if the Device is lost, stolen, or the Department considers that the Device's location is unknown to me, this will constitute an information security incident under the *Information Security Incident Management Policy* and must be immediately reported to my line manager **AND** the IT Service Centre.

Staff member initial here
Page two of three

17. I will immediately notify the Department if I become aware of any actual or anticipated unauthorised disclosure or use of any Departmental Information in connection with the Device, and I will take all steps that the Department may reasonably require in relation to such unauthorised disclosure or use.
18. I agree to the use of a remote wipe function if the Department suspects the Device is lost or stolen, and I acknowledge that this may include the permanent deletion of non-Departmental Information, data and intellectual property on the Device.

Release

19. I acknowledge that the Department accepts no responsibility or liability for, and I release the Department in relation to, any loss, cost, expense, or damage (**Liability**) incurred by any person, including me, where the Liability is related to, associated with, or connected to:
- a. a breach of any of these terms and conditions;
 - b. the use of the Device;
 - c. any non-Departmental Information on or accessed via the Device;
 - d. any action or omission of the Department in wiping the Device;
 - e. any combination of these circumstances.

Signed (staff member)

____/____/____
Date

Page three of three

Requestor's Name	
Business Unit	
Group / Division	

(please print)