

APPENDIX 5: IT Checklist

This checklist is intended to be advisory only. The following checklist is designed to assist departmental administrators, building managers, divisional IT teams or IT managers to ensure that IT and networking in a given building is operationally ready for a return to on-site working. It is expected that this checklist, not all of which will be applicable in every case, will be used in conjunction with other University guidance on preparing for a return to on-site working.

Check	Confirmed	Notes
If a building was previously closed, inform IT Services of the date from which the building is to be re-opened (help@it.ox.ac.uk).		Where IT Services has a role we would appreciate at least five days' notice of a building re-opening. IT Services will check: <ul style="list-style-type: none"> network connection and other monitored network services are functioning as expected Frodo UPS operating as expected.
Network infrastructure		
If maintenance work has been undertaken in the lockdown that might have impacted the network, inform IT Services or unit's IT support team, as applicable.		For IT Services, contact networks@it.ox.ac.uk .
Check that power is available to rooms housing network/server equipment and that UPS systems are operating as expected.		
Check that air cooling systems are operating in network/server rooms.		
Confirmation received from IT Services that network connection to building and related services are functioning as expected.		
If workspaces have been rearranged and different data ports now used, check with IT support team that all data ports are live or if changes to network patching are required.		In buildings where the <i>internal</i> network is managed by IT Services (networks@it.ox.ac.uk), it may take up to five days to fulfil network patching requests.
Check that networked devices that may have been moved are still on the correct network (especially in buildings provided with more than one subnet).		In buildings where the <i>internal</i> network is managed by IT Services (help@it.ox.ac.uk), relocated devices may require re-registering on the network.

Building online checks		
Confirm as per the Estates guidance that building management system (BMS), meters, fire alarm (SmartWatch), CCTV, and door access controller are online and functioning.		
Review any access control changes implemented in response to the lockdown.		Be aware that some University Cards may require re-enabling for door access control.
Check Chorus critical phones can make calls.		Faults with Chorus critical lines should be raised with help@it.ox.ac.uk in the first instance.
Login to a PC and access external web page.		
Make and receive call on Chorus deskphone.		Faults with Chorus phones should be raised with help@it.ox.ac.uk in the first instance. Common phone error codes are at https://help.it.ox.ac.uk/chorus/error-codes
Connect to eduroam and/or local wireless network with device previously known to work.		Contact local IT support team in first instance to report problems with building wifi services.
Check space and equipment booking systems, and visitor sign-in systems, are configured in line with new working practices.		
Workstations		
Identify workstations and other IT equipment that may have been taken home for remote working, and which will require returning and re-installing.		See also the items under working environment below.
Confirm that security updates have been applied to workstations previously switched off, relocated, during lockdown, or not receiving updates for another reason.		Time should be allowed for updates to be applied given that they may have accumulated over the period of the lockdown. Successful application of updates may require manual intervention at various points in the process. Some workstations will require a physical visit, others may be managed remotely (once powered on).

INTERNAL USE ONLY

Confirm anti-virus software (e.g. Sophos) is running and current.		See endpoint security, including Sophos installation, https://help.it.ox.ac.uk/security/endpoint
Confirm network drives are mounted and files accessible as expected.		Access to files may have been re-configured for remote working.
Check printers are online, toner and paper available.		
Working environment		
Ensure changes to working practices for IT support are communicated to IT team and users alike.		Consider and provide briefings for any IT staff who may be called upon to do a site visit to operational buildings. Ensure remote support remains in place (IT Services recommends Bomgar for remote IT support, https://help.it.ox.ac.uk/help/bomgar).
If applicable check that desktop PC users have a safe means of moving data between home and office environment.		Files and other data created or changed during lockdown may need to be transferred to departmental file storage or similar. One Drive for Business is a viable option for the transfer of data between locations (https://unioxfordnexus-my.sharepoint.com/).
Consider the need for files and other facilities to remain accessible for both on-site and remote working, including where shared by teams split between locations.		
Assess the extent to which workstations (including in meeting rooms and laboratories) are equipped with webcam and audio facilitates suitable for online meetings.		University preferred suppliers for IT peripherals are XMA & Insight Direct (https://finance.admin.ox.ac.uk/computer-supplies-and-services#collapse1146941). IT Purchasing Group has been asked to consider feasibility of central procurement of peripherals.
Check guidance for the use and cleaning of shared IT equipment, including workstations and touchscreens. Consider whether additional equipment, or workarounds, may be required to help minimise sharing.		