Client Device Local Administrator Rights Policy v1.1

Policy statement

Where necessary for the performance of a user's role the University shall grant colleagues administrator logon rights on Windows and Mac-based computers. If you have an existing device and would like to request a local administrator account, please do so using this form.

These rights allow you to:

- install software
- modify system settings
- manage other users of the device.

It is important that when using your local administrator account, you adhere to the following guidelines to protect the University's systems, devices and network:

- maintain the integrity and security of your workstation by not taking excessive risk by installing software from the internet
- always work whilst logged into your standard, non-administrative user account and only use the local administrator account to elevate privileges at the time when you need them
- ensure you do not grant administrator privileges to your standard user account or any other person's account or domain
- provide IT Services with licensing information for any software personally installed, Brookes owned or otherwise, on your device
- routinely check that your anti-virus software is updating, checking for and eliminating spyware, or any similar data gathering and reporting software, from your workstations
- do not share your local administrator account details with others
- report any system failures and security issues to IT Services at the earliest opportunity
- keep up-to-date with, and adhere to, all IT policies including, but not limited to, the IT Acceptable Use Policy
- do not interfere with any automatic updating/patching or enforced policies or services performed or provided by IT Services.

The University recognises that by giving colleagues administrative rights and enabling you to manage your workstations, productivity and operational efficiency can be substantially increased. However, Administrator access to a computer can lead to unintended and unauthorised configurations that may cause both you and the IT support service difficulties operationally and potentially legally.

Support for University devices

All University-owned devices that have access to the network, either wired or wireless, are required to be configured to the following standards:

- the device must be a member of a recognised university domain or management system
- the device must have the current required management software installed including, but not limited to, power management, software compliance toolsets, configuration management toolsets. (Management software may vary by device type)
- the device must have active, current and correctly configured anti-virus software
- the device must be patched with operating system and third party vendor patches to a level required by IT Services.

Any customisation of a device to a configuration other than that provided or supported by IT Services will be lost in the event of a computer failure. Its restoration will be to a standard pre-customisation configuration.

Staff responsibilities

The University reserves the right to restore a machine to a standard configuration if that machine is found to be a security risk. In such cases the University will not be responsible for any resultant data losses.

The University reserves the right to decline requests for administrator rights on any device for which access must be restricted due to its function, location or use by multiple users.

Misuse of administrator rights is defined as, but not limited to:

- downloading software that is malicious, by intent or otherwise
- downloading unlicensed/illegal software
- downloading and/or distributing copyrighted material without permission
- permitting public, or unauthorised, access to data that is restricted in nature
- failure to adhere to the policies and procedures outlined above.