Securing Imperial College

As the college moves towards more flexible hybrid ways of working there is an increasing need for data on the security posture, asset and inventory of devices accessing Imperial’s network, systems & data.

How do we do this?

This is done via tools such as [JAMF Pro for Macs](https://www.imperial.ac.uk/admin-services/ict/self-service/computers-printing/staff-computers/device-management/apple-device-management/) and [Endpoint Manager / SCCM for Windows devices](https://www.imperial.ac.uk/admin-services/ict/self-service/computers-printing/staff-computers/device-management/windows-device-management/) that validate the security posture and configuration of devices such as tablet computers, laptops and desktop.

Why do we do this?

Our institutional responsibilities for managing information and data security have become more stringent and are key for our work in obtaining Cyber Essentials certification. At the same time, with the advent of hybrid working, the scale and sophistication of criminal and malicious cyber-activity is increasing.

This will allow the organisation to exercise the required due diligence which must be undertaken in line with UKRI’s Principles on [Trusted Research and Innovation](https://www.ukri.org/about-us/policies-standards-and-data/good-research-resource%20hub/trusted-research-and-innovation/)

There are further benefits to utilising these tools such as a more consistent user experience, increased levels of support and faster issue resolution in case of security threats.

More specifically:

1. Speed of device delivery: Devices ordered from approved suppliers can go straight to the desired user rather than having to go through ICT, with the final configuration done by the user. This can save weeks in the process.
2. Consistent College authentication for all type of devices: The computer account is tied to Azure AD, which is the same as your college account, so the long-term goal is to make all services single sign on (SSO) and hence one account for everything.
3. Enhanced security: If security threats are detected, device management will allow faster remediation. In case of theft, it will also allow faster action.
4. [Cyber Essentials certification](https://www.imperial.ac.uk/admin-services/ict/about-ict/leadership/governance/certifications/): Cyber Essentials is a certification designed to show that an organisation has minimum level of protection in terms of Cyber Security. In order to achieve this certification, ICT needs to have the ability to have all critical or high rated security updates installed within 14 days and anybody accessing organisational data needs to be compliant. Having the certification will save time in filling research funding documentation and potentially attract new funding.
5. Consistent and improved level of support for all users: ICT aims to provide support for the purchase, set up, and renewal of the College's computing hardware and software. Device management for Windows as well as Mac devices will allow us to make sure the level of service in that area is improved especially for Mac Users.
6. Enterprise level support: In case of issue being reported, ICT can remotely fix the issue for a number of devices at the same time rather than individually accessing each machine.
7. Improved application support: If you have any issues installing or using any services provided by ICT, the support can be obtained centrally.
8. Better device compliance / Enhanced update and support: ICT will ensure that devices are up to date and in line with latest data and device policy so you don't have to proactively ensure compliance.

What level of management?



Currently exceptions are requested via the Service Desk, we are working on improving this process to streamline these types of requests and also agree the approvals required for exceptions.

\*Updates may not be fully applied until a reboot is completed (some take effect without a reboot)

We are aware that exception may need to be applied e.g. machines running long jobs or devices connected to lab equipment.

FAQ

For frequently asked questions on Apple device managed, go to:

[Apple Device Management | Administration and support services | Imperial College London](https://www.imperial.ac.uk/admin-services/ict/self-service/computers-printing/staff-computers/device-management/apple-device-management/)