Project EOS
The future of end user provision at Glasgow
Eos, (Greek), Roman Aurora, in Greco-Roman mythology, the personification of the dawn.

Named to reflect a new start in an area we have all been in for a long time.
New Demands

• In response to the changes precipitated in part by Covid, and more broadly by developments in technology and changes to our Estate Project EOS is our technology response to **enabling new ways of working**.

• As part of our response to these challenges we are going to take the opportunity to **significantly improve our security provision** and posture in recognition of the increasing threat to the University and its reputation by cyber criminals.

• These improvements are delivered by a range of **new services** that help the University manage the risks of these new ways of working, whilst delivering improvements to user experience across our whole estate.
What is it?

• Project EOS is a **suite of projects** to deliver a new range of support services for end users devices. Once delivered these services will become the default way to support end users and their devices.

• These new services securely support the **end to end life cycle for end user devices** from procurement to disposal, for both **Mac and PC** using self service.

• Mac and PC, Desktop, laptop and tablet are supported – **laptops are the default provision for all**.

• Project EOS is the first step in our journey to **next generation security provision**.
EOS

DEVICE SELECTION AND PROCUREMENT

DEVICE REGISTRATION AND CONFIGURATION

DEVICE ISSUE AND MANAGEMENT

DEVICE RETRIEVAL AND RECYCLE

DEVICE REPORTING AND MONITORING
Services

- Our new ways of working require a **laptop first approach** (although EOS does fully support all form factors in the end user space).
- **MyDevice** supports **PC Laptop device management**.
- We will support **Mac** devices fully, with a new **MyMac device management service** which will provide a full set of management tools for the MacOS and iOS platform.
- We will offer a **Software Asset Management Service** with end to end software procurement, packaging for all platforms and license management and reporting.
- We will offer a **Device and peripheral procurement service** with lifecycle carbon reporting and management.
- We aspire to attain **Cyber Essentials Plus** accreditation on all device platforms (SSD and MyDevice already passed, MyMac to be soon).
User Journey - Notes

• EOS provision, MyDevice (PC), MyMac (MacOs,iOS) is a **personal** device allocated to a single user and is not intended for shared use.

• The principle is to give the user a device which can do all the workloads required of it, precluding the need to issue multiple devices for multiple situations. This device is supported in University spaces via ubiquitous usb-c enabled docking to ensure large monitor support and better ergonomics.

• There are shared use models for scenarios where this is appropriate and they will continue to be supported. These services such as SSD, CSCE, AVD and Laptop Loan also come under the EOS banner and also benefit from the same improvements detailed in this presentation.
User Journey

• A user will select their device, Mac or PC from a set of options tailored to them in a portal, options can include any device available from any framework for designated users.

• Upon selection we will procure the device for them and it will automatically be registered in our inTune or Apple School Manager system.

• The device will be supplied to the user (from our stores where common parts kept in stock, or direct from vendor where not) to wherever the user wants to onboard*.

• The device is enrolled (Mac or PC, laptop, desktop or tablet) using the OOBE and your GUID credentials, behind MFA.
User Journey

• The device is now built for the user, using a tailored build and is ready to go (15 mins wireless).

• Users can request software via the helpdesk and once approved the relevant software will be added to their device automatically.

• 3 months before the device becomes 4 years old we contact the user to arrange for the provision of a replacement device and ensure the swap over of devices at the correct time.

• We then downcycle or dispose of the device with full carbon reporting.
User Journey

- Non role based devices land with Office, **OneDrive for storage**, Zoom and some plugins and the full security suite (Mac and PC).

- **Teams** for shared filestore, no access natively to SSD shared drives (Glasgow Anywhere for access).

- New software added by user using either a tool (such as software centre) or via helpdesk.

- **Admin** escalation can be requested allowing user to escalate to admin when required on device.

- Line of business applications supported via **Glasgow Anywhere**.
The technical details

• Every device is registered in our Azure AAD, and managed via inTune/SCCM or by JAMF.
• We have A5 licensing from MS so run the full A5 defender suite on Mac and PC and have real time reporting back to SIEM, with full integration to our Cyber team. Authorised clients for security scanning (Rapid7).
• JAMF provides Mac support for single sign on (JAMF Connect), application deployment and device management.
• Software asset management client for real time reporting.
• Cyber Essentials Plus accreditation for SSD, MyDevice now, and MyMac soon.
The biggest challenge to security in the end user fleet is the number of *unmanaged* devices which connect to it every day.

Unmanaged devices are unknown threats, and the number of them interacting with our services every day mean we are only able to use the minimum in controls in accessing our data.

Improving this position is a top priority for the University in Security terms.

EOS will move us to a place where we can consider implementing *conditional access*. 
• EOS will move us to a place where we can grant access to:
  • devices we know about (because we bought them and have an up to date asset register)
  • that we know are patched. (because we manage them)
  • that we know are free from malware or other signs of compromise. (because we have agents locally installed monitoring them)
  • that have credentials that make sense, and are coming from a time and place that make sense. (because we record and baseline their actions in our SIEM)
• That in summary meet the conditions required for safe collaboration.
  • This moves the perimeter of our protection to the end user devices, away from the servers and services that for legacy reasons carry vulnerabilities that we would rather place behind a firewall. This is a very significant increase in our ability to secure our network.
• By ensuring we procure devices, we can ensure we maintain an accurate device manifest. This allows us to adopt zero trust networking when the NIIP delivers the capability. Known devices access the corporate network, unknown devices treated as public.

• All EOS clients (SSD, MyDevice, MyMac) will have the full A5 MS Defender suite installed, connected back to our Security team monitoring toolkits. This is a significant upgrade to our existing provision.

• Local authorised agents for security scanning on all EOS devices.

• Our “out of domain” model for end user device provisioning significantly reduces the threat landscape to our critical business systems.
Software Asset Management

• A central service to procure, package & install, and manage software assets. Once packaged software can be accessed from any of our platforms, physical or virtual where licenses permit.

• Any software, Mac or PC, licensed by the University will be added to our Enterprise Software Library. Once in the library IS will provide contract management for renewal and license management, including reporting on license consumption within the fleet. We can import and manage locally procured software too.

• This service includes technology specific expertise from partners to advise on configurations to get the best deals from MS, Oracle, Adobe and others.
Procurement service

• A tailored device enrolment service offering each user a tailored view of an agreed University manifest of devices and peripherals many of which will be retained as stock items.

• Any device can be procured with college clearance, assistance can be devolved to local teams for device specification mapping.

• For non stock items the full range of options, from all of our suppliers and frameworks will be presented as options.

• Everything procured via this route is automatically added to hardware and software asset registers.
As with SSD there are devolved admin roles for MyDevice and MyMac.

Depending on user a dynamic mechanism to grant devolved admin, with the permission of the user, will allow local support teams to continue to support devices issued centrally.