Imperial College London

Returning to Campus Working Group

24 June 2021

Harbhajan Brar and Neil Alford

Imperial College London

Agenda

Time	Item	Purpose	Lead
10:00 – 10:30	Update on workstreams	• People • Safety • Technology • Space	AF, SJ, JV, SB
10:30 – 10:35	Frequency of meetings	To agree future frequency of meetings	HB
10:35 – 10:45	Future calls for evidence	To discuss future calls for evidence to aid the medium to longer term plans	JC
10:45 – 10:55	Communications	Standing item - agreement of which actions to communicate following this meeting and return to campus date	VS
10:55 – 11:00	Any other business	Standing item	ALL

Imperial College London

People Workstream

Update

Imperial College London

People Workstream update

The People workstream held its second meeting on Friday 19th June and:

- Finalised its **Terms of Reference**.
- Reviewed outputs from the **Call for Evidence** relating to people and hybrid working.
- Reviewed outputs from the **Wellbeing Surveys** in September 2020 and February 2021 to review over-arching trends in respondents' concerns about returning to campus. In particular, the change between the two surveys was reviewed (e.g. notable increases or decreases in responses).

The next People Workstream meeting on Wednesday 14th July will:

- Drill-down into clear trends from Wellbeing Surveys – Commute and Safety.
- Explore micro-coaching as a technique for managers to practice in the hybrid working environment.
- Discuss its proposed outputs (as per the Terms of Reference).
- Welcome departmental representatives into the workstream.

Imperial College London

Wellbeing survey – Returning to Campus

A useful set of qualitative data has been gathered from the September 2020 and February 2021 wellbeing surveys.

When asked '**What concerns do you have, if any, about returning to campus?'**

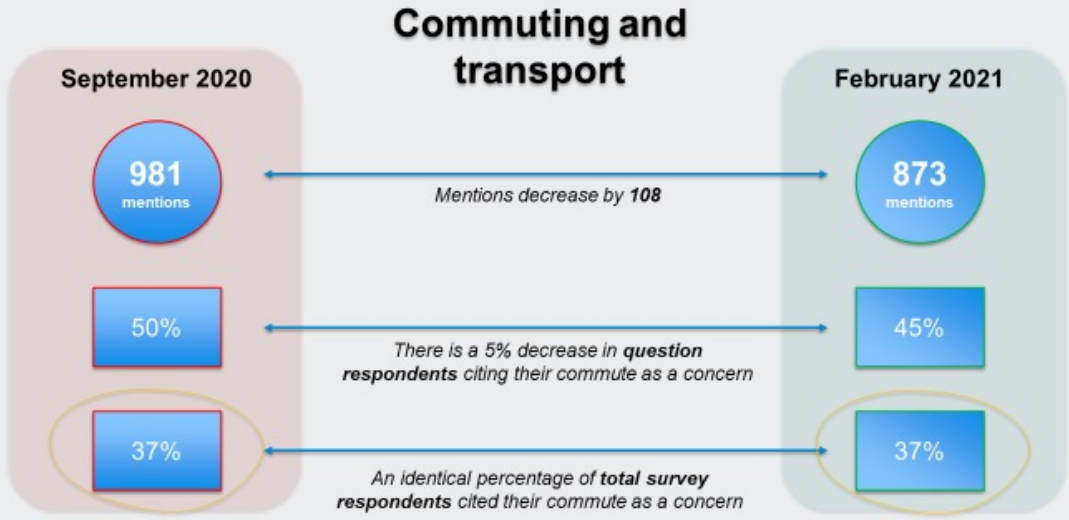
- **1,925** written responses (from **2,646** respondents) were received in September 2020
- **1,926** written responses (from **2,389** respondents) were received in February 2021

The following slides contrast mentions of **commuting & transport**, **safety**, **social distancing**, **mental health**, **workload** and **technology**, to show the change in perception between the two surveys.

The number of mentions is contrasted against both the total written responses (i.e. of those who wrote an answer, X mentioned this theme), and the total number of responses received (i.e. of those who filled out the survey, X mentioned this theme), to ensure that the data is considered in both contexts.

Imperial College London

Wellbeing survey – Returning to Campus



NB: a full-size slide is annexed to this deck

Commuting and transport

The most frequently-occurring concern in both surveys is the commute. Further analysis will be done to separate:

- Those who are raising a concern about commuting due to **health and safety**, meaning "I am at greater risk of contracting COVID-19 if I commute."
- Those who are raising a concern about commuting due to **work/life balance, productivity or workload**.
- Other commute concerns.

Imperial College London

Wellbeing survey – Returning to Campus

Safety

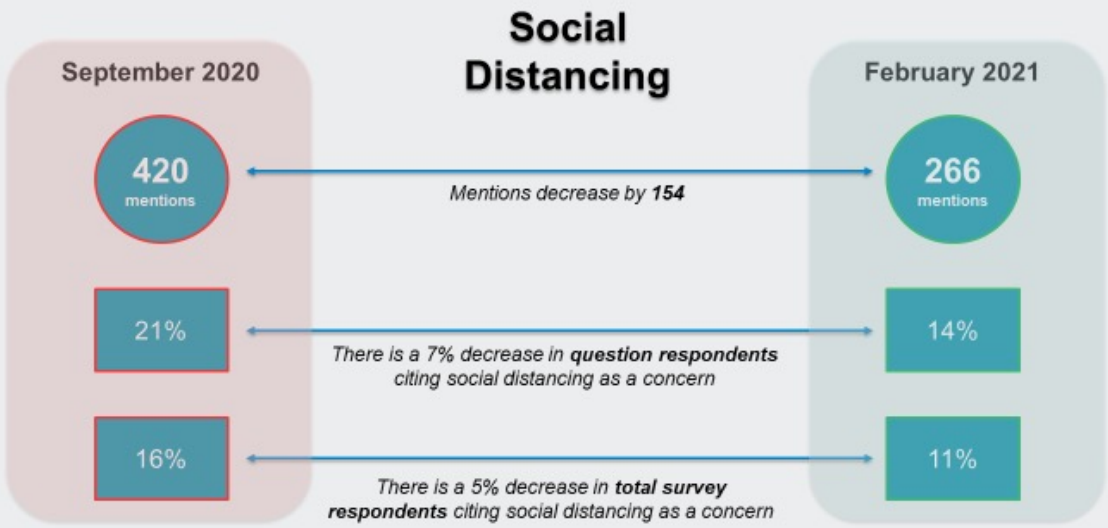
There is a slight increase in the number of respondents citing Safety as a concern, making it a common trend

Further analysis will be undertaken on these responses to determine the specific cause for concern (e.g. ventilation, cleaning and hygiene, etiquette).

NB: a full-size slide is annexed to this deck

Imperial College London

Wellbeing survey – Returning to Campus



Social distancing concerns

No further analysis will take place, however the number of respondents citing social distancing as a concern **notably decreases** between September 2020 and February 2021.

NB: a full-size slide is annexed to this deck

Imperial College London

Safety Workstream

Standing agenda item; Safety roadmap here.

Imperial College London

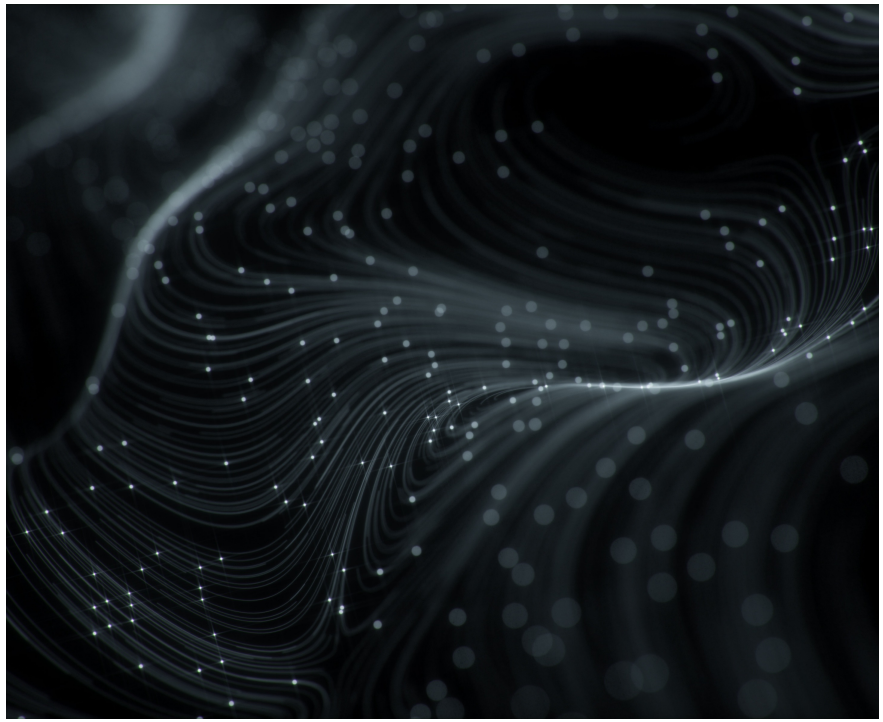
Technology Workstream

Update

Return To Campus Working Group

24/06/2021

Secure, flexible working at Imperial



Imperial College London

Background

- Part of the Vision for a World Class ICT Function is to provide an enhanced and consistent user experience that supports the College in being a world leader in research and teaching.
- This transformation requires systems, services, application programming interfaces, data and processes to be accessible through multiple mechanisms anywhere, anytime, from any user device over the internet. This provides a greatly improved user experience but also expands the surface area for attackers to target with our current solutions.
- Therefore, we need a new security model that more effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects people, devices, applications, and data wherever they are located. We are addressing this challenge and the ever growing cyber threat risk by introducing a new "Zero Trust" security model which will provide greater protection for systems in the new world of remote teaching, learning and research.
- The core of the “Zero Trust” security model is to never trust anyone from either within or outside of the corporate network, always verify, the user, the endpoints (these could be college owned and managed, BYOD, contractor, partner or guest devices) and the applications that run on them.
- This is a huge step change as at Imperial we are still heavily dependent upon On Premise applications (Around 90% of our 600 services are hosted in our Data Centres) that are largely secured via network zones, as data travels between each zone it passes through the firewall and the associated set of rules and is accessed remotely via VPN.
- Not all endpoints are managed or even owned by Imperial meaning we have a variance of devices, operating systems, configurations and software patch levels. This along with the health and trustworthiness of the applications that run on those endpoints impacts both our security posture and the user experience.

Imperial College London

Zero Trust Benefits for Imperial

Zero Trust solutions treat all connections as untrusted, regardless of where the user and their device are coming from, until automatic security validation has taken place, making access more secure than it is today.

Zero Trust also provides better control, faster breach detection times and greater insight into network access and activity to help better protect our environment.

Other key benefits of Imperial adopting a Zero Trust strategy:

- **Secure access -** with Zero Trust policies users can only access resources they are permitted to and applications can only communicate with specific devices which in turn have to match a defined set of standards in terms of operating system level, patches and anti virus definitions. This secures Imperials applications and the data they hold.
- **Supports flexible working -** users can access their applications from any device in any location removing the need to be on campus all the time or the need for multiple devices.
- **User centric -** Zero trust provides a more simplified log in process. Everything happens in the background, and the user doesn't have to sign-in to multiple applications; users will simply use their existing log on account.

Imperial College London

Visibility of devices accessing our services and their status

There will be minimum security compliance rules which either prevent access until remediation activities have taken place or provide limited access to specific applications.

The same security policies will apply whether the device is owned and managed by ICT or BYOD (Bring your own device), whether it is accessing via our network, home broadband, or the public internet and whether the service is on premise or is provided by SAAS (Software as a Service) or PAAS (Platform as a Service).

We will provide our users with modern portable devices that will give them a consistent user experience and allow them to work wherever they need to rather than being tied to a desktop on campus.

Imperial College London

What's next & how you can help

The starting point for delivering Zero Trust is to create user role profiles.

We are determining who our users are, what role they play within our organisation and what applications they need to access. This will enable us to create user roles aligned to:

- Faculties & Departments
- Teaching & learning
- Research
- Estates, Campus & Commercial
- Finance & HR
- ICT Operations
- External stakeholders

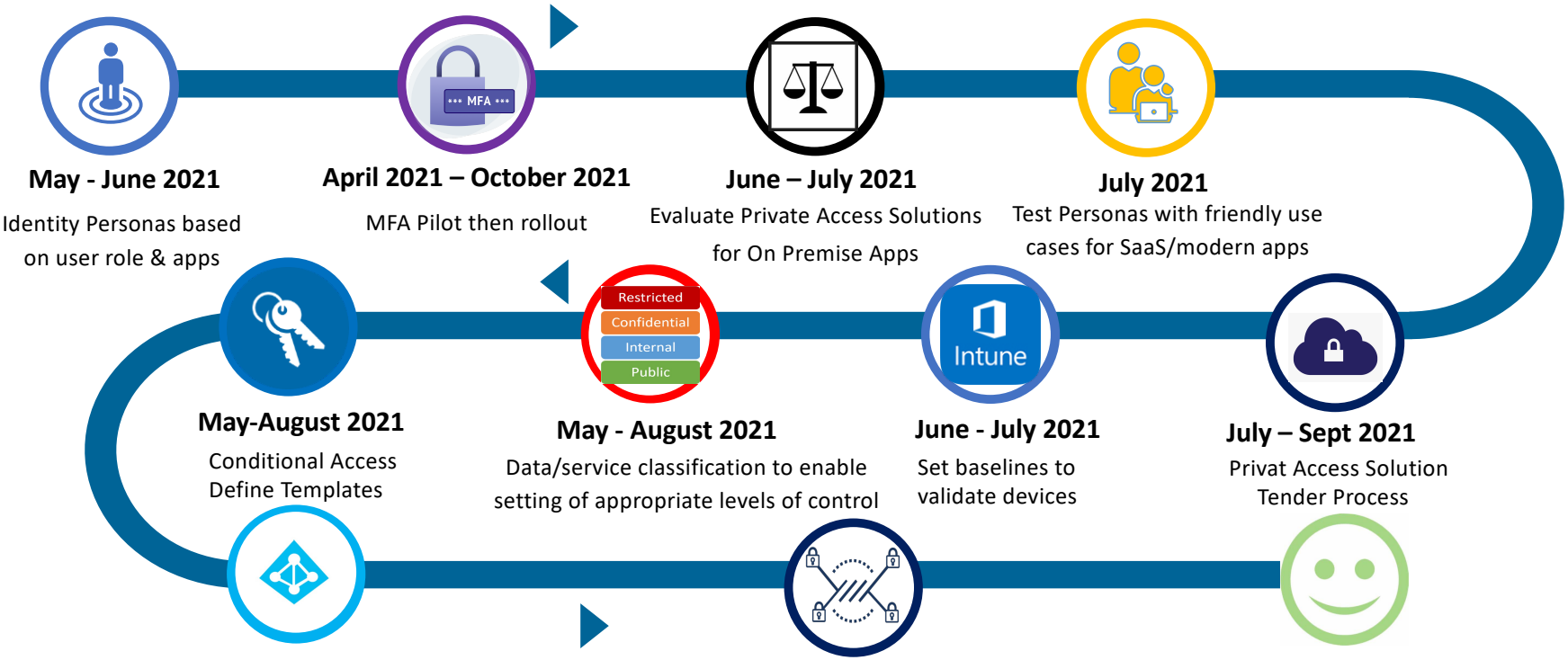
For the current phase we are starting to validate these user roles with you and your teams so if you haven't already heard from us we will be getting in touch to kick off this process

This will allow us to ensure we have a clear understanding of what applications each department need access to for their role along with the level of access required

The Roadmap for Zero Trust is on the next slide, the key areas we will be working with you on are steps 1 and 4.

Imperial College London

Timeline for Zero Trust



May - June 2021

Identity Personas based on user role & apps

April 2021 – October 2021

MFA Pilot then rollout

June – July 2021

Evaluate Private Access Solutions for On Premise Apps

July 2021

Test Personas with friendly use cases for SaaS/modern apps

May-August 2021

Conditional Access Define Templates

May - August 2021

Data/service classification to enable setting of appropriate levels of control

June - July 2021

Set baselines to validate devices

July – Sept 2021

Privat Access Solution Tender Process

March - December 2021

Migrate SAML apps authentication to Azure Active Directory & config Shibboleth to consume

Sept – March 2022

Deploy private Access Solution to remaining On Premise services

April 2022

Users access apps from any device & location securely

Imperial College London

Key Milestones

Milestone	Activities Status	Target Date
Define User Persona	User persona draft template is ready. Interviews with Business School, Digital Lab, FOE (Faculty of Engineering) Research, FOE Computing Manager have been scheduled and are in progress.	Complete Ongoing
Discovery Of applications and Data flows	Creation of discovery questionnaires for information on network data flows and discovery of applications. Network discovery underway to identify how to obtain traffic flows from endpoints.	29/06/2021
Collated data set documenting all known data flows.	This activity is dependent on discovery phase, documentation will start once all data is available based on discovery questionnaire. Further detail will follow once discussions undertaken with Network Lead- Mark Carter.	06/07/2021
Documented assessment of application and data flows across	This activity is dependent on technical discovery of application and data flows which is underway. Documentation will start once data is available after discovery phase.	13/07/2021
Discovery and baselining of connected devices (EUC) and assessment against NCSC principles.	Discovery questionnaire for end user devices being created.	20/07/2021
Review of technical infrastructure to identify gaps and opportunities against NCSC Zero Trust principles, including identification of required Architecture Building Block enablers for Zero Trust	Vendor assessment for private access solution is in progress and call for tender process with Commercial team is scheduled for next week.	31/07/2021

Imperial College London

Zero Trust & Laptop Benefits for Imperial

The combination of implementing our Zero Trust solution along with rolling out Laptops to users instead of Desktops provides further overall benefits to the college:

- **Better facilitates hybrid working and collaboration** Mobile allowing access from any location compared to Desktops which require remote desktop access and additional devices for off campus access.
- **Onboard technology to secure** device tools like BitLocker and other security features in Windows 10 via TPM ensures data is secured & access restricted to only the users who should have it
- **Creates more flexible use of campus space** College is space constrained. Using laptops would enable hybrid/smart working and would make space available for teaching/research
- **Native Biometrics** Desktops can be enabled with biometrics but these are additional peripherals which are built into Laptops
- **Reduced Power Usage** College desktops are often left on to connect remotely. Due to issues with networking machines often don't wake up so are left on. Power is wasted here but also at home where a 2nd device is used.
- **Can be "locked" into College ownership** College assets can be secured so they can't be reloaded outside of College
- **Can access "on-prem" services remotely** Currently requires VPN for laptops. BYO devices are being used otherwise (via VPN).
- **Secure within a location** Lockers can be used to store overnight on campus
- **Can be shared amongst different users** Future thinking around putting shared laptops into Laptop Lockers would mean devices could be shared between groups. This would be useful if the laptop had particular requirements / geo-fenced for data protection reasons
- **Touch capable (using right model)**

Imperial College London

Space Workstream

Update

Imperial College London

Space workstream update

Since last RTC meeting

- As part of licence renewal process, it is anticipated that LoneRooftop will be extended to the Faculty Building, Dyson Building, Chemistry 4, 5, 6 and Scale Space (Business School areas).
- Set-up of Sherfield and Faculty building working groups complete.
- Answering queries to reinforce the messages that Safety guidance is key, there are no central drivers for more staff on campus or central policing of “rules” and that this is a period for learning.

Next steps

- Review of questions for the next call for evidence survey to enable collection of more granular information on anticipated use of space.
- Consider what information we would like to gather during the Transition and Learn phase and which data sources will be useful.
- Regroup and refresh on room bookings, including a review on where we are with Planon and future opportunities, and a re-look at Celcat Room Booker and the SALC rooms to agree next steps.

Imperial College London

Frequency of meetings

To agree future frequency of meetings

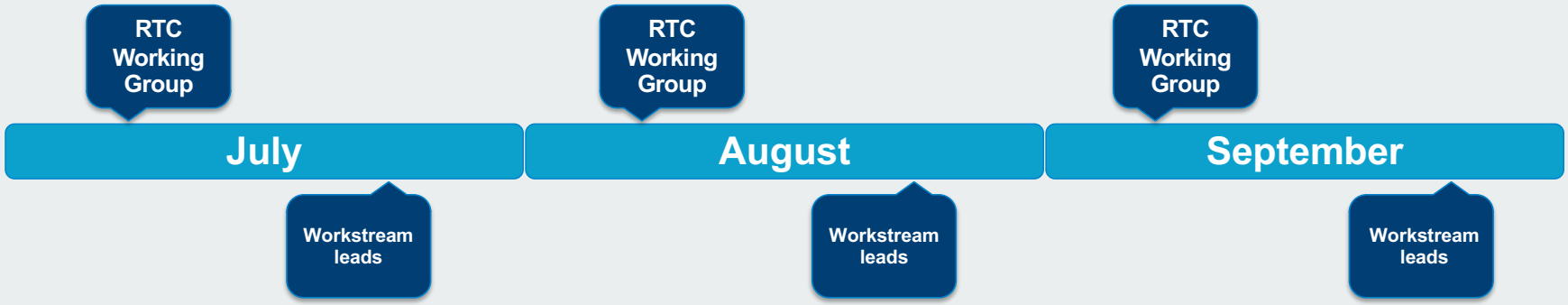
Imperial College London

Proposed meeting frequency

The Returning to Campus Working Group currently meets fortnightly, which was an appropriate frequency while its scope and workstreams were being established.

It is proposed that the organisation of the Working Group changes:

- The Returning to Campus Working Group meets **monthly.**
- The Workstream Leads meet monthly, in the place of the second Working Group meeting, to ensure an agenda is clear for the Working Group, share planned work, and discuss any workstream-interdependent activities.



Imperial College London

Future calls for evidence

To discuss future calls for evidence to aid the medium to longer term plan(s) to return to campus

Imperial College London

Future Calls for Evidence

Following Calls for Evidence in February (informal, via email) and April/May (formal, survey), information gathered directly from departments has been vital in informing the Returning to Campus Working Group and its workstreams' activities.

Detailed Call for Evidence – TBC, likely July/August 2021

- Separates types of staff in responses – Academic, Research and PTO – for clearer reporting
- Adds detail after high-level Call for Evidence in April/May – plans will likely be firmer
- May require multiple respondents per department

Shorter Call for Evidence following the start of autumn term – November 2021

- Assumed to be short and structured as questions 'by exception' – e.g. "Have you changed your working arrangements as students return to their studies"
- Medium – survey or otherwise – to be confirmed based on appetite of RTC Working Group.

Longer Call for Evidence in January 2022

- What approaches, particularly relating to Space and People, are departments going to keep (e.g. long-term hybrid working or space-sharing arrangements)?

Imperial College London

Communications

- Standing agenda item

Imperial College London

Any other business

- Standing agenda item