Crown
Commercial
Service
Supplier

huddle™

Multi-Agency Collaboration in UK Government

How teams use technology to work across agencies, public sector bodies, and private sector partners

Covering Central Government, Local Government, NHS

July 2020

INTRODUCTION

It has been six years since the Home Office shared findings from its 'Multi-Agency Working and Information Sharing Project'[1]. The findings offered a unique look into the multi-agency information sharing models being adopted across UK government and called for agencies, public sector bodies, and private sector partners to work together in a way that improved decision making, quality of service, and cost.

In practice, many public sector stakeholders found this push towards greater collaboration challenging; not least because of a lack of shared IT infrastructure, but also poor cloud and security awareness.

So where are we today, six years after that important call to action?

External collaboration is now a necessity

Since the publication of the project's findings, those in Central and Local Government, as well as public sector services such as the NHS, have witnessed seismic changes to the way they work.

Whether it be through greater private sector partnerships across the NHS, or more complex Multi-Agency Safeguarding Hubs (MASH) spanning local authorities, and a variety of support services, collaboration beyond the firewall is no longer a choice, it is a necessity.

This demand has been supported by a huge rise in the availability of cloud-based apps and systems designed to improve collaboration. However, it's also been accompanied by a rise in security threats and a general feeling of complexity – both in the breadth of stakeholders involved in multi-agency projects, but also the volume of content that needs to be shared and worked on.

To better understand the challenges, Huddle commissioned a study spanning more than 600 public sector employees, comprising 307 from Local and Central Government, and 301 from the NHS[2]. The goal of the study was to better understand the technologies being used for collaboration across organisational firewalls, how users are adapting to changes in working practices, the challenges they face, and the awareness of today's mounting security risks.

Executive Summary

For government and public sector teams, collaboration beyond the firewall is no longer a choice, but a necessity.

regularly collaborate with stakeholders outside of their own organisation

feel they have been adequately trained to use the apps available to them

say they can't work with external stake-holders because of incompatible apps and IT policies

feel that their IT security policy makes it too hard to collaborate externally and across agencies

Security compliance is also a concern. Familiarity with the Government's Security Classifications has improved, but not enough.

21%

very familiar with Government Security Classifications

34%

not at all / not very familiar with Government Security Classifications

admit to using personal file sharing apps to share and collaborate on files

[1] Multi-Agency Working and Information Sharing Project: https://www.gov.uk/government/publications/multi-agency-working-and-information-sharing-project

[2] Interviews were independently conducted for Huddle by Censuswide, during Q1 2020

WORK HAS CHANGED, BUT OLD HABITS DIE HARD

Today's work is not confined to organisational borders. In fact, 55% of respondents routinely share files and collaborate with stakeholders outside of their organisation.

However, despite the changes to who we need to work with, the most prevalent tool for how files are shared remains familiar; email.

This is trailed by organisation's using their own file sharing system (or apps like Huddle) (26%), document management platforms such as Microsoft OneDrive (24%) and Microsoft SharePoint (17%), and Enterprise Messaging apps such as Microsoft Teams (12%). (Fig.1)

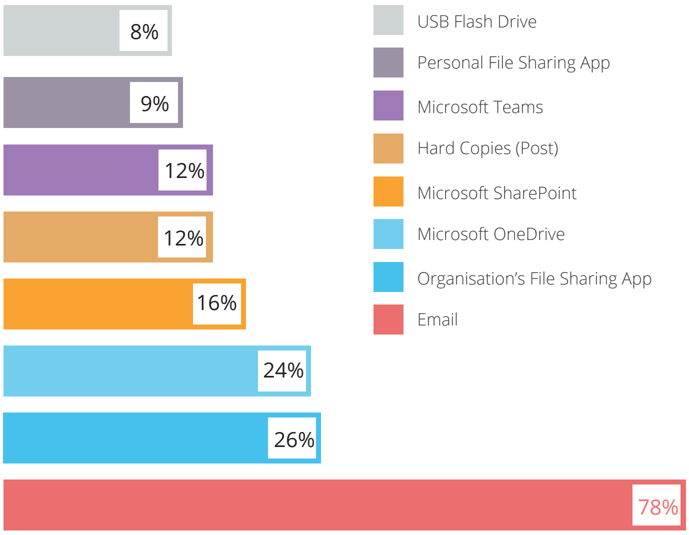


Fig 1. Which apps do you regularly use to share and collaborate on files (internally or externally)?

Unfortunately, despite the growing availability of mandated cloud-based platforms, many respondents are still using less secure mothods of information sharing.

12% are still regularly sending hard copies of documents via the postal system or a courier network and worryingly, personal file sharing apps and USB flash drives (9% and 8% respectively) are yet to be eradicated from the workplace.

What's wrong with email?

The pervasiveness of email helps to position it at the top of the list of apps most commonly used for sharing and collaborating on files. However, for working across a distributed group of stakeholders it is a cumbersome tool and likely remains a favoured choice only because of the deficiencies seen in other collaborative technolgies, or continued firewall restrictions.

Infact, many of email's limitations are realised on a daily basis by respondents.

- Loss of version control: Sending materials as attachments can create unnecessary version control problems, with stakeholders each creating separate working versions of a file. 15% of respondents cited loss of document version control as one of their most frustrating collaboration challenges. (Fig.3)

- Lack of visibility: Tasks and updates can quickly become buried in lengthy email threads. This makes it hard to maintain visibility and keep track of the latest updates. 19% stated that a lack of visibility, leading to a duplication of effort, was a common cause of frustration and delay. (Fig.3)

- Email is not secure: 91% of cyber-attacks and data breaches begin with an email. In fact, more than half of respondents (57%) have received an email phishing attempt to their work email address. Sharing files via email also means that the file "owner" loses control of the document. This means it can be forwarded-on and shared beyond its intended distribution list, or copied and saved on devices and apps that do not meet the organisation's minimum security requirements.

MANY APPS STILL FAIL TO MEET THE DEMANDS OF EXTERNAL COLLABORATION

Respondents were asked about their use of several popular Microsoft apps, including Microsoft OneDrive, SharePoint and Teams (Fig.2).

While these apps have a solid user base for internal file sharing and collaboration use cases, their ulilty declines for multi-agency and external collaboration use cases.

The drop-off in usage for these apps externally may be explained by some of the common challenges respondents cited:

- Restricted by IT security policies: 19% said that their IT security policy makes it too difficult to share and collaborate on files with people outside of their organisation. Given that apps such as Microsoft Teams are predominantly built for internal users, IT policies will often default to limiting their use beyond the organisational firewall.

- Different systems: 19% said that the people they needed to collaborate with work within organisations that used different apps and systems. Often this is not a feature restriction (apps such as Microsoft Teams will offer a "Guest" mode), but instead an IT policy decision designed to ensure sensitive information is not compromised.

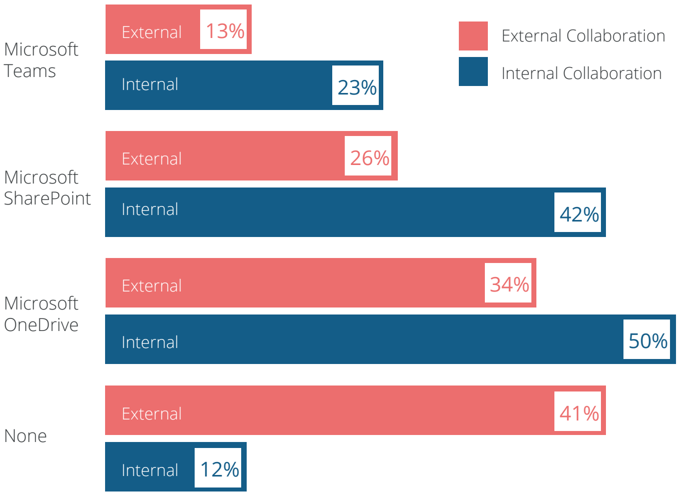


Fig 2. Which of these apps do you use to share and collaborate on files

- **Too many options:** 21% said that they have several cloud options for saving and sharing files (OneDrive, SharePoint, etc), and find it confusing to determine which to use for internal vs external sharing (Fig.3). This is becoming a common complaint as organisations continue to expand on their tech-stack and progress through their digital transformations. Users become paralysed with the complexity and number of options available to them, typically then defaulting back to email.

Shadow-IT

Unfortunately, it is challenges like these that continue to fuel the use of shadow-IT (describing the use of apps and services that don't meet approved security standards and typically break an organisation's security policy).

When mandated file sharing and collaboration tools don't meet the individual's use case (for example, collaboration outside of the firewall), many will look to find their own solutions.

External User Limitations of Microsoft Teams

Just 13% of government and public sector employees use Microsoft Teams when working with stakeholders beyond the firewall.

It's use for external collaboration can present a number of challenges.

- Non-federated, guest access can be hard to control. Guests will have access to all channels within the team (unless set to private), creating potential security risks.
- External, guest users are not able to search for saved files.
- Microsoft Teams' audit trail is limited to O365 admins only, making it hard to track user and file usage.
- Guests are identified by their email address. This can sometimes make it hard to identify them. Display names can only be edited by your O365 admin.

In this instance, 9% admit to regularly using a personal file sharing account (i.e. Dropbox), and 8% admit to using unencrypted USB flash drives. Both of these come with serious security risks, and leave the organisation unable to build an audit trail of document usage.

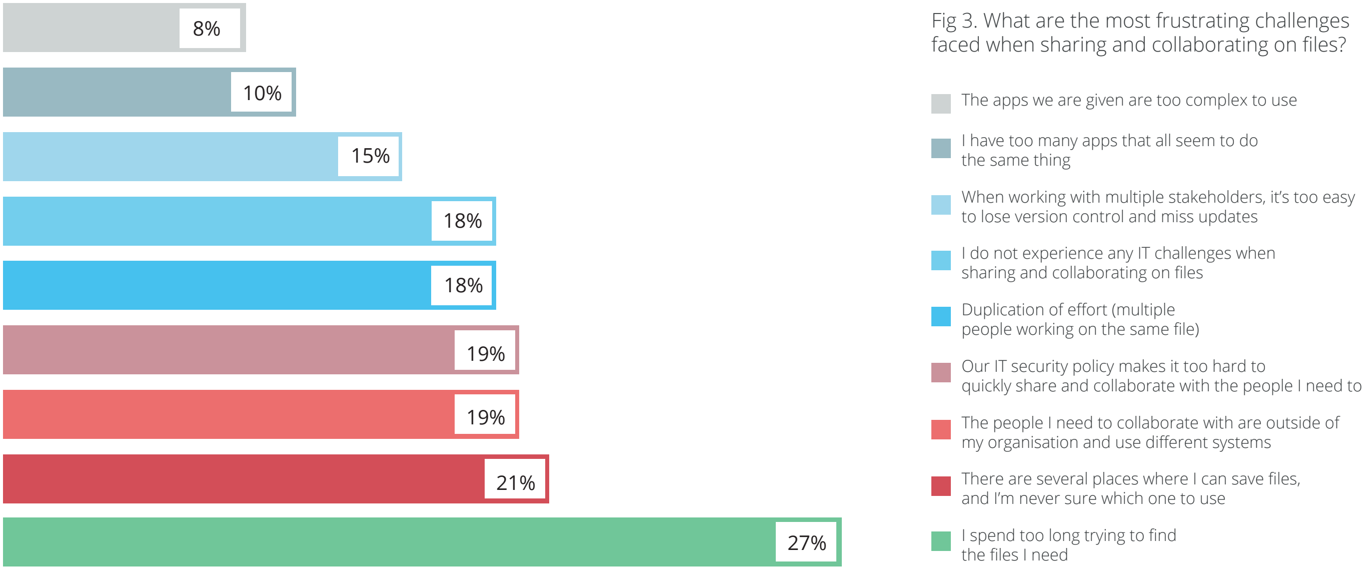
COMMON COLLABORATION FRUSTRATIONS

Despite efforts to improve the way these organisations collaborate, common pain points remain. (Fig.3)

Digital distraction

The availability of more and more apps and services to support collaborative use cases is overwhelmingly positive. However, there is a potential concern that IT leaders should familiarise themselves with; too much choice can lead to complexity and confusion for their end users.

Fig 3. What are the most frustrating challenges faced when sharing and collaborating on files?



As a result of using different apps to store and share information, 50% of senior executives are spending anything up to 30 minutes each day simply searching for, saving and sharing files; and 25% of them admit to never being sure where to save their files (a challenge shared by 21% of the entire base of respondents).

- Unsurprisingly, the lack of file availability is a common cause of complaint across all respondents. 27% agree that they spend too much time searching for files. (Fig.3)
- 10% went as far as saying the apps available to them all seem to do the same thing. (Fig.3)
- 8% feel that the apps they have access to are too complex and confusing to use. (Fig.3)

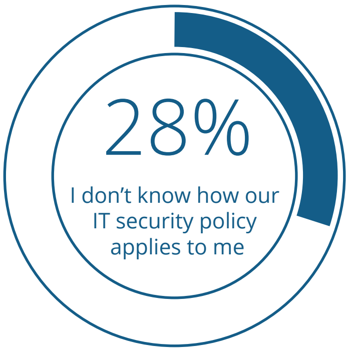
KEEPING EXTERNAL COLLABORATION SAFE AND SECURE

Through any period of digital transformation, it's important that adequate training is given to users. This can assist in overcoming many of the common complaints highlighted by this survey. Most notably the 8% that feel that the apps they have access to are too complex, the 21% that are not sure which app to use, under which circumstance, and even the 19% that feel IT security policies make it too restrictive to work externally.

Unfortunately, IT training remains a weak point across many government and public sector organisations. Just 17% felt they have been adequately trained, and that the training materials they have access to are completely sufficient. Over a quarter (29%) feel that training was not at all, or not very, sufficient, and the remaining 55% feel it was only somewhat sufficient.

Security awareness

Training should include not just the functional aspects of the tools, but also how existing IT policies apply to them. Today, security training appears to be routine, with only 7% unsure if a security policy even exists within their organisation. However, whether the available security policy is understood is questionable – more than a quarter (28%) said that despite being aware of an existing security policy, they are unsure how it relates to their role.



Government Security Classifications

When Huddle conducted a similar survey in 2014, the level of familiarity around Government Security Classifications was low and particularly limited outside of Central Government. At the time, less than half of IT professionals (48%) within Local Government were aware of how documents should be classified.

Familiarity has since improved. Today, 67% of all respondents are somewhat familiar, or very familiar, with the Government's most recent security classifications.

Surprisingly, awareness was below average for senior executives (58%), the cohort most likely to be working on sensitive documents. Awareness was also low among younger age categories, with just 56% of under 34 year olds showing awareness of how document confidentiality should be classified. (Fig.4)

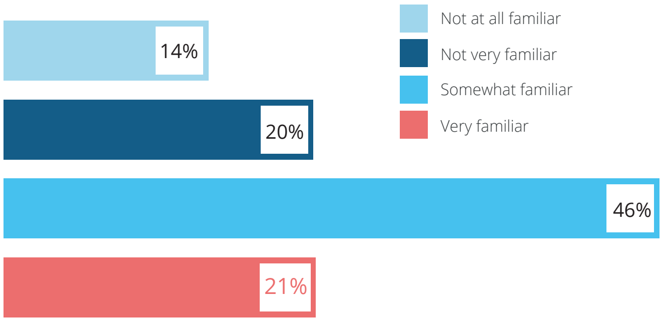


Fig 4. How familiar are you with the latest Government Security Classifications for the handling of files and data?

SUMMARY

Government and public sector workers are routinely working with stakeholders from other agencies, local authorities, and even private sector partners.

While organisations have undergone a period of digital transformation to enable this change, many of the apps and services available to employees still aren't meeting their needs for external collaboration.

Security

The majority of respondents are aware of their organisation's IT security policy. However, many continue to use shadow-IT (such as personal file sharing apps and USB flash drives) to circumvent restrictive policies. Alternatively, they rely on email, which can pose its own security (and productivity) risks.

At the other end of the spectrum, a growing number of users have access to tools such as Microsoft Teams and Microsoft SharePoint. However, the use of these apps is largely for internal use cases. External use is either blocked by IT, or limited by the apps' own functionality.

Damaging Productivity

Productivity issues feature prominently in the list of common IT challenges. The most frequently cited complaint was that it takes too long to find the files that users need. 34% of respondents admit to spending more than one hour per day simply searching for, saving and sharing files.

Much of the issue comes from poor version control, with files being shared as email attachments. This can result in multiple copies of the same file, attachments being saved locally, and updates being buried in lengthy email chains. 15% feel that version control is too easily lost, adding to complexity and duplication of effort.

Meeting the needs of new employees entering public sector and government roles

Traditional mean of working with external stakeholders (like email) are being rejected by younger employees, who instead favour more transparent and collaborative apps. This same cohort of users are also the most vocal about restrictive IT policies, suggesting that the availability of collaborative apps still isn't meeting their needs.

MULTI-AGENCY COLLABORATION WITH HUDDLE

The need to deliver better services, and at a lower cost, is driving every level of Government to look for new, more collaborative ways of working.

However, one barrier remains: an integrated, shared IT system. It means that many agencies are still working in informational silos, hampering cross-agency collaboration.

As the most trusted solution for government and public sector bodies who need to improve multi-agency collaboration, Huddle knows that the challenge isn't as great as it might seem - and not nearly as expensive as many of the legacy solutions being operated today.

Collaborate safely across the firewall

Government agencies and their partners often need to come together to deliver major projects. This typically requires agility and coordination of effort around a large volume of documentation.

However, with participants from an increasingly broad spectrum of organisations, project groups can often experience challenges caused by the lack of a shared IT infrastructure. In these scenarios, program delivery can be delayed and even compromised as participants default to less secure methods of sharing information.

Huddle provides a simple, yet highly secure way to connect internal teams with stakeholders outside of your firewall. Huddle works by allowing you to build customized project Workspaces where teams come together to work on files, exchange information, manage tasks, set approvals, and discuss updates.

And, because Huddle is cloud-based, it sits above your existing IT infrastructure so you can be sure everyone has access. Being cloud-based also keeps everyone synchronised to the latest files, so there's never any risk of out-of-date information being shared.

Trusted by:

Department
for Environment
Food & Rural Affairs

Department for
Business, Energy
& Industrial Strategy

Home Office

Cabinet Office

Foreign &
Commonwealth
Office

Ministry
of Justice

UN
environment

World Health
Organization

huddle™

huddle.com

UK
2 Leman Street
London
E1 8FA

U.S.
535 Mission St
San Francisco
CA, 94105

U.S.
4500 East-West Hwy
Bethesda
MD, 20814

South Africa
151 Campground Road
Newlands
Cape Town, 7700