General Apps Guidance

# General Apps Guidance

## Overview

When working from home, you still need to communicate with Ministry of Justice (MoJ) colleagues. You'll also need to work with people outside the MoJ. There are various tools you might use, besides the standard email and telephone tools. This document tells you about the tools you can, and cannot, use for business purposes. This guidance applies to all staff and contractors who work for the MoJ.

Some ALBs, Agencies, or other large groups within the MoJ might have their own, specific guidance regarding how to use certain Video and Messaging apps for different purposes.

## Access to tools

You can access tools that are provided through your MoJ provided devices by downloading from:

* The Software Centre application on your device (for Dom1 equipment).
* The Self Service application on your Mac (for Digital Service Desk (DSD) managed MacBook laptops).

Currently, access to the tools mentioned in this document is not available from Quantum devices.

For other MoJ provided devices, seek help from your Line Manager in the first instance.

## Corporate, work and personal accounts

* A corporate account is for making official MoJ statements and providing official views. Only a small number of authorised people can use it.
* A work account is your normal MoJ account, that you use every day for business as usual. Only you have access to your work account.
* A personal account is your own personal account on gmail, hotmail, yahoo, and so on. You should never use a personal account for business purposes.

Some of the applications listed make a distinction between general use with a work account, and use with a corporate account. Using a tool with a corporate account means you are providing views or statements on behalf of the MoJ. Never use a personal account for business purposes with any tool.

Remember that if you are authorised to use a corporate account, you are speaking and acting for the whole of the MoJ. When working with a personal account, you are speaking and acting as an MoJ employee and a civil servant.

Always follow all [MoJ policies and guidelines regarding public information, including social media (to access this information you'll need to be connected to the MoJ Intranet)](https://intranet.justice.gov.uk/documents/2015/11/social-media-policy-guidance.pdf). In particular, follow the [Civil Service Code of Conduct](https://www.gov.uk/government/publications/civil-service-code/the-civil-service-code).

## Using video conference tools safely

The NCSC has excellent guidance on [using video conferencing services safely](https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely).

Key things to remember *before* a call include:

* Make sure your video conferencing account (or the device or app you are using for video conferencing) is protected with a strong password.
* Test the service before making (or joining) your first call.
* Understand what features are available, for example recording the call or sharing files or screen information.

Key things to remember for *every* call include:

* Do not make the calls public, for example always require a password to join the call.
* Know who is joining the call, in particular check that everyone is known and expected to be present, and that people who have dialled in have identified themselves clearly and sufficiently.
* Consider your surroundings, for example checking what can be seen behind you (forgetting to check information on a whiteboard or noticeboard is an easy mistake).

## MoJ Policy and guidance

### OFFICIAL and OFFICIAL-SENSITIVE Information

OFFICIAL information is the majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

OFFICIAL-SENSITIVE is not a classification. SENSITIVE is a handling caveat for a small subset of information marked OFFICIAL that requires special handling by staff. You should apply the handling caveat where you wish to control access to that information, whether in a document, email, or other form.

### Privacy and personal information (Data Protection)

Some communications tools expect to have a copy of your contacts list. The list is uploaded to the tool server in order to let the tool to function correctly. Think carefully about whether this is reasonable to do. Make sure that sharing your contacts list does not impact any one else's privacy in a negative way.

Data protection legislation makes you responsible for personal information you work with. You must keep it safe and secure. In particular, you must follow data protection obligations. These include the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Complying with personal information requirements can be complex. Don't hesitate to ask for advice:

* Email: [privacy@justice.gov.uk](mailto:privacy@justice.gov.uk)
* Slack: #securityprivacyteam
* Intranet: <https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/>

### Information Management

Many of the tools are only used for your day-to-day communication with colleagues. The information you work with is typically [classified](https://www.gov.uk/government/publications/government-security-classifications) at OFFICIAL.

Think about the MoJ information you work with when using these tools. What would happen if you lost your mobile device, or it's stolen? Suppose the voice or video call was overheard in a cafe, or read from your screen on a crowded train. Could there be damaging consequences? If the answer is 'No', then it's probably OK to use the tool to communicate that information with colleagues.

You have a duty of confidentiality and a responsibility to safeguard any HMG information or data that you access. This is [Principle 2](https://www.gov.uk/government/publications/government-security-classifications) of the Government Security Classifications. The MoJ trusts you to work with OFFICIAL information. You're trusted to make a reasoned judgement about whether it's safe to use an approved tool, or whether you should use a different MoJ-provided work tool.

Remember that it is impossible to delete information after it's released in public.

For more information about MoJ IT Security, look on the MoJ Intranet [here](https://intranet.justice.gov.uk/guidance/security/it-computer-security/).

### Storage and data retention

Laws and regulations make the MoJ and its employees responsible for managing information. Some examples include:

* Freedom of Information Act.
* Data Protection Act and General Data Protection Regulation.
* Public Records Acts.

When we receive a request for information, we need to know where we hold all the relevant information. Storing business information on appropriate MoJ systems helps us, because:

* We can provide evidence about decisions.
* We understand the information held, and where to find it.
* We can transfer records to The National Archives.

Always store MoJ information in MoJ systems. If you use a tool for work tasks, make sure the key information is stored in an appropriate MoJ system. Guidance on what you must keep is available on the Intranet [here](https://intranet.justice.gov.uk/guidance/knowledge-information/managing-information/what-to-keep/). At regular and convenient intervals, transfer the information to an appropriate MoJ system. Do the same when you finish the work. Don't forget to remove any redundant information from a tool by clearing or deleting data if it has been preserved in an MoJ system.

Many tools lets you export your data. You can then store it on an appropriate MoJ system. Sometimes it's easier to copy and paste text into a new document. Make sure that only the correct people have access to the information. This is important after staff or organisational changes, for example.

For more guidance, read the [MoJ Information Management Policy](https://intranet.justice.gov.uk/documents/2015/04/information-management-policy.pdf) on the Intranet. There is also help on [responding to requests for information](https://intranet.justice.gov.uk/guidance/knowledge-information/providing-information-to-the-public/freedom-of-information/).

## Acceptable Use

You must use communications tools for business purposes in an acceptable way.

Be sensible when using communications tools for MoJ business purposes:

* Be extra careful with sensitive and personal information in tools.
* Try to avoid using the same tool for business and personal use - you can get confused who you're talking with.
* If the message you're about to send might cause problems, upset, offence, or embarrassment, it's not acceptable.
* Context is important - a message you might think is funny could be upsetting to someone else.
* If something goes wrong, report it.

The bottom line is: *"if there is doubt, there is no doubt - ask for help!".*

## Approved tools

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tool name | Tool type | Conditions/ constraints on use | Accessing /installing tool | Audience |
| Apple Facetime | Communication tool: Video | Avoid personal or sensitive data | Smartphone App | Internal/External |
| Apple iMessage | Text messaging | Avoid personal or sensitive data | Smartphone App | Internal/External |
| Google Meet (was Google Hangouts) | Communication tool: Video and/or voice | MoJ use approved | Digital Service Desk controlled Mac - Self service, Web browser. | Internal/External |
| Microsoft Teams | Communication and collaboration tool: Video and/or voice | MoJ use approved | Dom1 Software centre, Digital Service Desk controlled Mac - Self service, Web browser. | Internal/External |
| Miro | Collaboration tool: Whiteboarding | Avoid personal or sensitive data | Web browser. | Internal/External |
| Skype for Business | Communication tool: Video and/or voice | MoJ use approved | Dom1 Software centre, Digital Service Desk controlled Mac - Self service, Web browser. | Internal/External |
| Slack | Text messaging, Voice/Video calls, etc. | Avoid personal or sensitive data | Digital Service Desk controlled Mac - Self service, Web browser. | Internal/External |
| Slido | Q&A tool during presentations | Avoid personal or sensitive data | Web browser. | Internal |
| Twitter | Text Messaging, Video transmission | Approved for MoJ Corporate account. Using a personal account to comment on work related issues is encouraged, as long as you follow the [Civil Service Code of Conduct](https://www.gov.uk/government/publications/civil-service-code/the-civil-service-code). | Web browser, Windows 10 App, Smartphone App. | Internal/External |
| WhatsApp | Text messaging, Voice/Video calls | Avoid personal or sensitive data | Dedicated app on device, also web browser. | Internal/External |
| Yammer | Text messaging | Avoid personal or sensitive data | Dedicated app on device | Internal |
| YouTube | Video sharing tool: Video, streaming and chat | Avoid personal or sensitive data | Web browser based use. | Internal/External |
| Zoom | Communication tool: Video, voice and chat | Avoid personal or sensitive data | Web browser based use | External meetings |

## NHS Track and Trace

The official [NHS Covid-19](https://www.nhs.uk/apps-library/nhs-covid-19/) app was designed by the NHS. Both NCSC and Cabinet Office have been involved in the security of the system. The app provides contact tracing, local area alerts and venue check-in. It enables you to protect yourself and your loved ones. Installation is optional, but recommended.

After installing the app, you'll receive an alert if you have been in close contact with other people who have tested positive for coronavirus. You can then take action to avoid passing the virus on, for example by self-isolating.

From a security perspective, it is safe for you to use the app on your personal or MoJ issued devices. There are no extra risks for colleagues with security clearance, such as SC and DV.

If you wish to install the app, start at the [NHS site](https://covid19.nhs.uk/).

Note: The NHS app may not work on some older MoJ devices. Installation might not be possible, for example on Quantum smartphones.

You might have both a personal and an MoJ issued device. Think about which device makes most sense to use with the app. It's best to install on the device that you carry with you and use most of the time. You could install on all your devices if you prefer.

To reduce the likelihood of false alerts on the app, turn off the app's Bluetooth mode. Do this when:

* You are working in environments with protective Covid measures in-place, for example plexiglass separators.
* You need to leave your personal or work device in a locker, for example during a sports activity or to work in a secure MoJ facility.

## Other tools

Some tools, such as Facebook, Instagram and LinkedIn, are approved for specific corporate accounts to use, for corporate communications messages. General use of these tools for work purposes is not permitted.

If you wish to use a tool that is not listed above, please consult our [Guidance for using Open Internet Tools](guidance-for-using-open-internet-tools.html) and [speak to us for help](mailto:security@justice.gov.uk).

## Requesting that a tool be approved for use

Refer to the [Guidance for using Open Internet Tools](guidance-for-using-open-internet-tools.html) for the process to follow when wanting to add a new tool to the list.

## Other information

### Government policy and guidance

[GDS Social Media Playbook](https://www.gov.uk/guidance/social-media-playbook)

### NCSC

[Video conferencing services: using them securely](https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely)

[Secure communications principles](https://www.ncsc.gov.uk/guidance/secure-communication-principles-alpha-release)

[Using third-party applications](https://www.ncsc.gov.uk/collection/mobile-device-guidance/using-third-party-applications)