#Open internet tools

**This information applies to all staff and contractors who work for the Ministry of Justice (MoJ).**

##Overview

Open Internet Tools (OITs) are applications or services from suppliers outside the MoJ. They often have the following characteristics:

* they are general purpose. This means they are not specific to the MoJ. Other organisations can use them
* they are accessed using the Internet, usually through a web browser. This means that if you have Internet access, you are able to connect to the tools
* they have a basic ‘free-to-use’ version. This means that you are able to use some or all the capabilities, but with some constraints. For example, an online word-processor might limit you to 5 documents in your account
* they have one or more ‘paid for’ versions. By paying for the tool, you unlock some or all the constraints

##Quick checklist

To help you decide if you can use an OIT to work on an MoJ task, consider the following questions:

* is the task information subject to specific rules or requirements in your part of the MoJ?
* is the task information classified as anything other than OFFICIAL or OFFICIAL-SENSITIVE?
* does the task information include any data identifiable as being about someone?
* is this the first time anyone has used the tool for MoJ business?
* does the tool need access to your account or other data you can access? For example, does it ask to use your MoJ Google or Microsoft Office account?
* does the tool install a web-browser extension?
* is the tool a plug-in for existing OITs we use, such as Slack, Confluence, or Jira?
* could there be damaging consequences if the task information you work with using the tool is:
  + lost
  + stolen
  + published in the media
* are you prevented from exporting all the data from the tool?
* are you prevented from deleting all the data from the tool when you finish working on the task?

If the answer to *any* of these questions is Yes, you might not be able to use the OIT.

When you have all the answers, request formal approval to use the OIT from your [Line Manager](/guidance/security/it-computer-security/line-manager-approval/). Do this *before* using the OIT.

##Why OITs are an opportunity

OITs offer some significant advantages for you and the MoJ, including:

* enabling you to work the way you want to, more effectively
* usually cheaper than buying or building and supporting a dedicated tool
* no need to build or support the tool
* good use of open standards, such as file formats
* reduced need to have specific hardware or software on computers
* rapid patching to address security issues
* easy updates and deployment of new features
* a large pool of help and support
* easy access, whenever you have a network connection
* increasing availability of some or all capabilities when disconnected from the network

##Why OITs are a risk

OITs also pose some threats or risks, including:

* dependency on the tool and supplier
* security of access to the tool
* security of information stored within or processed by the tool
* potential difficulty of enhancing or customising the tool for MoJ-specific requirements

But as long you consider the threats or risks, and address them, OITs provide many benefits for you and the MoJ.

##Summary

With careful use, OITs help you to work more effectively and efficiently. Think about them as serious and preferable options for performing tasks.

##Using OITs

This guidance helps you:

* understand the conditions or constraints that apply to a tool, or a task performed using a tool
* identify and address threats or risks posed by a new tool

##Privacy and personal information

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).

Don’t use OITs for storing personal data until you have addressed the need to get consent first. Check if using the OIT might need an update to existing privacy policies or notices. Don’t use OITs if unlawful disclosure of the information they process might cause damage or distress.

Data protection legislation might also limit *where* you can process personal data. An OIT should have a privacy statement that describes where it stores or processes data. Be ready to contact the OIT provider for more information about this aspect of their service.

Be sure you can fulfil your data protection responsibilities when using an OIT. It might be helpful to complete a [Privacy Impact Assessment (PIA)](/guidance/knowledge-information/protecting-information/privacy-reform/data-protection-impact-assessments-dpias/).

Complying with personal information requirements can be complex. Don’t hesitate to ask for advice: [privacy@justice.gov.uk](mailto:privacy@justice.gov.uk)

##Classification and security

An OIT can only store or process information [classified](https://www.gov.uk/government/publications/government-security-classifications) at OFFICIAL level.

Think about the MoJ information you work with. What would happen if you lost it, or it’s stolen, or published in the media? Suppose the information 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 OITs to store or send that information.

Think also about information moving across the Internet. The data might be safe within the MoJ and in an approved OIT. But what about the connection between the two? Sending information might involve insecure networks. Be aware of the security implications. Check that enough suitable security measures are in place to protect the information. For example, check for encryption of network connections using [SSL/TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security). A simple way to do this is to look for the secure connection indicator in your web browser:

The image shows a small section from a web browser URL bar. The word ‘secure’ appears in a green color, to show that the connection is safe. There is also a padlock icon in a closed state, again to show that the connection is safe.

The image shows a small section from a web browser URL bar. The word ‘secure’ appears in a green color, to show that the connection is safe. There is also a padlock icon in a closed state, again to show that the connection is safe.

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. In the same way, you’re trusted to make a reasoned judgement about whether it’s safe to use an OIT.

Useful help for deciding what is OK is in [existing social media guidance](/documents/2015/11/social-media-policy-guidance.pdf). While it’s more about how to act online, the principles are helpful for OITs.

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

More information can be found on the [MoJ IT & Computer Security](/guidance/security/it-computer-security/) pages.

##Storage and data retention

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

* the Freedom of Information Act
* the Data Protection Act and General Data Protection Regulation
* the 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 an OIT, make sure the key information is also stored in an appropriate MoJ system. Guidance on what you must keep [is available](/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 the OIT.

Most OITs let 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](/documents/2018/01/information-management-policy-jan-2018.pdf). There is also help on [responding to requests for information](/guidance/knowledge-information/providing-information-to-the-public/freedom-of-information/).

##Service and support

OITs are often intuitive and reliable. But that doesn’t mean they are always available and always work as you expect. The MoJ can’t provide technical support or ensure service availability for them. Always have another way of working if the OIT is not available for some reason or for any length of time. In other words, don’t let an OIT become business critical.

Check the OIT usage agreement to find out more about the service and support available.

**Note:** The MoJ cannot provide technical support for OITs.

##Common OITs

There are already many OITs used across the MoJ. Permission to use an OIT might vary, depending on where you work in the MoJ. For example, some teams must not access or use some OITs, for security or operational reasons.

**Note:** Check with your Line Manager if you want to use an OIT for your work, *before* you use it.

##Requesting that an app be approved for use

If there is an application or service that is not currently approved, but which you would like to use, you can request a security review.

Begin the request by filling in the [Request a Security Review of a third-party service](https://docs.google.com/forms/d/e/1FAIpQLSeEEBDS1HBF7meUk3SjgkqxbXBQlKAiBAezJIbKHnEjfNjBTg/viewform?gxids=7628) form, as best you can. The more information you provide, the better. But don’t worry if you have to leave some bits of the form blank.

When you submit the form, it is passed to the security team. The app is reviewed, to check things like how safe it is to use, and whether there are any Data Privacy implications. The security team will respond to you with an answer as quickly as possible.

**Note:** You should submit the request, and wait for a formal approval response, *before* you install or use the app on MoJ equipment or information.

If you have any questions about the process, contact the security team: [security@justice.gov.uk](mailto:security@justice.gov.uk).

##Getting help

For further help about aspects of using OITs within the MoJ, contact:

|  |  |
| --- | --- |
| Subject | Contact |
| Classification and Security | [MoJ Cyber Security team](mailto:security@justice.gov.uk) |
| Storage and Data Retention | [Departmental Library & Records Management Services (DLRMS)](mailto:kim@justice.gov.uk) |
| Information Assurance | [Compliance and Information Assurance Branch](/guidance/knowledge-information/protecting-information/information-assurance-roles/) |
| Personal Data | [Disclosure Team](mailto:data.access@justice.gov.uk) |

##Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).