Ministry of Justice

ALPHA

Used with common sense, open Internet tools will be a powerful aid in helping you to work more effectively.

The Cabinet Office has published an introductory guide to some tools that may meet your needs, but there are many others out there, and many more yet to be built. By providing general guidance on using any such tools we hope to empower you to decide for yourself how you can work most effectively. Existing social media guidance focuses on how to act online when communicating in public. This guidance focuses on how to use online tools in your daily work.

Security

You can use online tools to store or transmit any MOJ information that would not have damaging consequences if lost, stolen, or published in the media. In short, anything that you would not mind being overheard in a cafe, or read from your screen on a crowded train is safe to store online. It is up to you to make a reasoned judgement.

Information management

As with all information you handle for work, when using online tools it is your responsibility to ensure that key information is also stored on the appropriate MOJ system. You can read guidance on 'What to Keep'. You may wish to designate someone on your team to make sure this happens.

Personal data

You are responsible under the Data Protection Act (DPA) for the security and stewardship of personal data in your care. We would advise that open Internet tools are generally unsuitable for the transmission or storage of citizens' data, unless their consent is gained; and always unsuitable for data that would cause damage or distress to an individual if disclosed, including sensitive personal data as defined by the DPA. Take particular care if you are handling citizens' personal data that you comply with the DPA; the data compliance team can advise on how to do so.

Service and support

While open Internet tools are designed to be intuitive and reliable, MOJ Technology is not responsible for providing technical support and ensuring service availability. Given that the department has no control over these tools, you should not use them in such a way as they become business critical.

You can use online tools to store or transmit any MOJ information that would not have damaging consequences if lost, stolen, or published in the media. In short, anything that you would not mind being overheard in a cafe, or read from your screen on a crowded train is safe to store online. It is up to you to make a reasoned judgement.

When you use online tools in the course of your work you will be transferring information over the Internet, and often storing it online. This happens outside the Ministry of Justice's (MOJ) IT systems so you need to be aware of the security implications.

Each person who works with government has "a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access" (Government Security Classifications April 2014).

The best online tools use industry standard security measures to protect your data. These include amongst other things using SSL/TLS, which secures data in transit, as recommended in the Government Security Classifications.

It is important you follow this guidance, as it can be difficult to delete information if it is released by mistake. For more information on IT Security, consult IT security guidance and policies.

As with all information you handle for work, when using online tools it is your responsibility to ensure that key information is also stored on the appropriate MOJ system. You can read guidance on what to keep. You may wish to designate someone on your team to make sure this happens.

Various pieces of statute mean the Ministry of Justice and its employees are responsible for managing information. These include the Freedom of Information Act, the Data Protection Act, and the Public Records Acts, amongst others.

Ensuring that you store records of significant business on appropriate MOJ systems fulfils your obligations under these pieces of legislation. It protects you and the Department by making it easy to provide evidence of why decisions have been made. It helps you and colleagues to understand what information is held, and where to find it if requested. It also enables the Department to transfer a carefully selected portion of policy and court records to The National Archives.

If a request for information is received you will need to consider where all relevant information is held. This can include information stored on open Internet tools if you haven't already transferred this to an appropriate MOJ information storage system. At the end of a piece of work, make sure that you transfer relevant information, and remove any redundant information from the tools.

Most tools provide you with an easy way to export your data which you can then store on an appropriate MOJ system. It may sometimes be easiest to copy and paste text into a new document. You should ensure that the right people have access to the information in case of staff or organisational changes.

For more information please consult the MOJ Information Management Policy and guidance on requests for information.

You are responsible under the Data Protection Act (DPA) for the security and stewardship of personal data in your care. We would advise that open Internet tools are generally unsuitable for the transmission or storage of citizens' data, unless their consent is gained; and always unsuitable for data that would cause damage or distress to an individual if disclosed, including sensitive personal data as defined by the DPA. You should take particular care if you are handling citizens' personal data that you comply with the DPA; the data compliance team can advise on how to do so.

The DPA imposes broad responsibilities on organisations to protect personal data and sets out definitions for personal and sensitive personal data. The Act stipulates that personal data can only be used for the particular purpose for which it was collected; this is explained in more detail here. The DPA also obliges organisations to take "appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." For in depth guidance relating to what this means in practice please consult ico.gov.uk.

A further requirement of the DPA is that "personal data shall not be transferred outside the European Economic Area (EEA) unless that country ensures an adequate level of protection". Some United States (US) companies also meet this "adequate level" if they comply with the US-EU Safe Harbor scheme. Most tools should make this clear in their Privacy Policy, but you may need to contact the company if it is unclear. When using a new tool, you need to ensure that you are fulfilling your responsibilities under the DPA.

There may be occasions when you process citizen personal data online – this could be when you crowdsource ideas when you run an Open Policy Making exercise, for example – but when doing so, you should consider the requirements of the DPA and any privacy risks by completing a Privacy Impact Assessment (PIA). Open Internet tools may not be suitable for the transmission or storage of large volumes of personal data but you may need to transmit or store small amounts to be able to use the tool effectively. For example, you may need to use the names of colleagues when assigning tasks in a tool like Trello. You should discuss this with your team to ensure they understand how their personal data will be used.

For more information on the DPA please visit ico.org.uk. You can find out more about MOJ's Data Protection responsibilities on the MoJ intranet.

While Open Internet Tools are designed to be intuitive and reliable, MOJ Technology is not responsible for providing technical support and ensuring service availability. Given that the department has no control over these tools, you should not use them in such a way as they become business critical.

Open Internet Tools are services provided online by third party companies. These companies depend on providing an easy-to-use and reliable service to retain their customers. In general, they provide clear and concise support documentation to help you get the most out of the tools they offer. They are generally available to use 24 hours a day, 365 days a year, with only occasional downtime for maintenance and improvement.

Because these services are offered outside of MOJ's Service Level Agreements with our existing technology suppliers, MOJ Technology is not responsible for providing support and ensuring that the services are available. You should consider how to use these platforms in the knowledge that if something goes wrong it is the tool supplier, rather than MOJ, who is responsible for helping you.

Many tools provide excellent support on their websites. In the unlikely event that the tools are not available, they malfunction, they lose your data, or you don't know how to do something, you will rely on support from the tool supplier to fix your issue. It is important to be aware that you may not always be able to speak to someone for help.

You may like to check the User Agreement of a given tool to find out more about the service and support it offers.