Guidelines on use of software and general computing resources provided by third parties (cloud services)

This advice relates to the use of software or filespace being offered by third parties. This is usually free or at very reduced cost but creates other concerns that should be considered. This advice will consider first the position of the user, then that of the department that may wish to utilise such products and provide them on to their users.

The jargon used to describe such offerings includes "cloud computing", "software-as-a-service (SaaS)" - examples are Google Docs, iCloud, Microsoft Onedrive, Amazon Web Services, Dropbox. It can also include providers of survey tools, such as Survey Monkey, and mail distribution websites, such as Mailchimp.

For the user who wants to take advantage of, possibly free, resources:

1) These resources - software or filespace - often reside on machines/disks that exist wherever is convenient for the service provider. This can change, often frequently, and data may be passed on to or through sub-contractors. More often than not, this is in the USA.

   QM has various obligations with regard to personal data covered by the Data Protection Act 1998 as outlined in the Data Protection Policy. Specifically, there are responsibilities for security and the restriction of that data to within the European Economic Area (or a small number of other specified countries, not including the USA).

2) You must be aware that these facilities usually come with little or no guarantee of availability - you should never use them as your only source of material - e.g. you should not keep your only copy of an important document on a third party disk or use third party software as your only means to get something done.

3) Your data may be encrypted in transit, but you need to consider its storage. Where is it held? Is it encrypted? Can foreign law enforcement agencies gain access to it?

   REMINDER: you should not use any web-based email, such as GMail or Hotmail, for conducting QM business.

For departments considering use of such resources, obviously the points above need consideration, but also:

4) Companies do get into trouble and there have been instances of companies failing and giving users little or no warning to rescue their own data.

5) Even though locally provided QM services can suffer problems, QM services are supported and QM takes all due care and consideration with regards to business continuity when there are problems. Data on College machines is appropriately registered with respect to the Data Protection Act so that QM is not liable to prosecution for breach of the DPA.
More compliant alternatives

In order to ensure that data remains within the EEA, there are a number of alternative suppliers which do the same thing as those which are based abroad or use facilities there:

- QM has an account with Bristol Online Surveys, see http://www.learninginstitute.qmul.ac.uk/elearning/support/survey/
- Wuala offers cloud storage and backup
- Dotmailer stores all information on U.K. servers

Relevant links: QMUL Data Protection Policy
QMUL Cloud Legal Project