University of Hertfordshire RDM Cloud Storage Review

Comparing popular cloud services to UH policy

Cloud storage has become a common solution to researchers back up and sharing requirements. In this document we review the most popular facilities analysing the pros and cons of their data and security policies as well as their costs and access.

Dr Joanna Goodger

Mrs Sara Hajnassiri

Dr William Worthington

JISC

Cloud storage

One of the trickiest aspects of research is assuring that your data is backed up, but also that it is secure whilst being easily shared with collaborators. In many research disciplines, data is in the form of confidential personal information, which may include medical data, proprietary data, or data which is patent pending.

In the past, many researchers have turned to cloud storage solutions to share their data between devices and/or collaborators. Cloud storage is a model of networked online storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centres, and people who require their data to be hosted buy or lease storage capacity from them.

For some service providers, much of the data which you have access to is not your property and you are saving your right to access it and not the data itself (e.g. icloud), while other companies can store whatever documents/data you upload to their servers; however, they also have rights to access and, in some case, use your data. What they have in common is that they do not accept responsibility for damages, corruption or loss of your files. They all advise you to keep your own backup of the data.

UH Policy

The University of Hertfordshire's research data policy states;

> ❝The University owns data generated by its research; it expects data to be managed and shared in a robust and professional manner; and it places the responsibility for proper research data management with the Principal Investigator.

While this might imply a proprietary or protectionist tone to the University's data policy, this is not the case. The University's data policy also has the following clauses from the main policy section that counter this impression:

4.2   The University recognises the value of data as an institutional resource and considers that value to be increased through the widespread and appropriate use of data and by virtue of data quality.

4.3   The University considers the value of data to be diminished through misuse, misinterpretation, or unnecessary access restrictions.

The use of third party cloud storage is thus is violation of the University's data policy as the third party hosting company has access to the data which you store and thus the ownership of the data is at risk. This is a major concern for private data and we recommend encryption of your data in all instances where you are sharing data.

UH cloud services

To avoid the mismanagement of your research data, we recommend using the UH storage services which allow you to share your data within and without the University without breaching the University's data policy.

However, if you have to use cloud storage due to collaboration guidelines, then we suggest that you **consider these issues**:

Who owns the data on your shared drive?

Check the Terms and Conditions as some providers take ownership of your data. However, most declare that you are alone responsible for your data and that you retain your intellectual property rights, but the rules change depending on where in the world your data is being held.

What is the back-up policy of the service provider?

Will your data be backed up daily, weekly, or monthly and are previous versions retained? Some providers will keep previous versions indefinitely, others for a month or not at all. You do not want an automatic synchronisation to override an important version of your code or report.

Can they suspend your account without notification?

The majority of providers reserve the right to close your account if they decide that you have misused it. If your research includes nude art work, photos and videos of children, music files, machinery CAD files, they may misinterpret your intentions as illegal and close your account. Files will likely be scanned by a robot that will analyse the files plainly and account closures may not be reversible.

Is your provider under obligation to disclose the contents to law enforcement or any other authority?

If your data is open to misinterpretation, the local law enforcement to the country where your data is stored may be notified so the consequents are greater than the closing of your account. You should consider your shared files with an air of caution; could they be misinterpreted as paedophilic, theft or an act of terrorism?

Can you store encrypted files?

If your research is sensitive, you may want to encrypt the files, but your provider may not allow encrypted files to be stored on their cloud service due to the suspicious nature of secretive data; you could be breaking the law and they could not analyse the contents.

Common Cloud Services

To highlight the advantages of using the UH Storage solutions for sharing data, we have compared the features of other popular sharing services, which were mentioned by staff during our enquiries[1].

Service	Cost	Formats	OS	Backup	Data Ownership / security	Other features/limitations
iCloud	Free for 5GB* $10 for +10GB $20 for +20GB $100 for +50GB	Media (music, film) Images* (photo, video) Messages* (SMS, MMS) Device settings* Documents*	Mac	Daily when on mains power and screensaver. Retains last 3 backups only.	Individual only, which expires on death and is non-transferable. Apple and third parties access user info.	
Policy highlights: http://www.apple.com/legal/icloud/en/terms.html Users will not "engage in any copyright infringement or other intellectual property infringement (including uploading any content to which you do not have the right to upload), or disclose any trade secret or confidential information in violation of a confidentiality, employment, or nondisclosure agreement;" "Apple does not claim ownership of the materials and/or Content you submit or make available on the Service." as long as you do not put it in a publicly accessible area. Data may be stored by third parties outside the UK and will then be subject to the host countries laws. * The 5GB of free storage excludes **purchased** music, film and TV, which is owned by iTunes. Un-purchased media is not backed up by Apple.						
DropBox	Free for 2GB – 18GB $9.99/month 100, 200, or 500GB 1TB for teams with shared billing.	Any file format. Images and video can be viewed using DropBox website.	Windows, Mac, Linux, iPad, iPhone, Android, Blackberry	Retains a one-month history of your work. Any changes can be undone, and files can be undeleted.	Share your data with other selected users. Secure Sockets Layer (SSL) and AES-256 bit encryption Data stored by Amazon S3.	Only updates are transferred between desktop folder and online storage. Manual set bandwidth
Policy highlights: https://www.dropbox.com/terms "You retain full ownership to your stuff. We don't claim any ownership to any of it. These Terms do not grant us any rights to your stuff or intellectual property except for the limited rights that are needed to run the Services". Dropbox and Amazon operate in the USA and are therefore subject to US law and FOI.						

---

[1] UH Research Data Assets Survey May 2012 http://research-data-toolkit.herts.ac.uk/2012/08/data-asset-survey-results/

Service	Cost	Formats	OS	Backup	Data Ownership / security	Other features/limitations
Google Cloud	5 GB (free) Pay as you Go. Charges for data stored, uploaded and downloaded. Billed annually. Unlimited > 400 TB+	Any file format	Mac, Windows	Users are responsible for the backup- (for Google Cloud SQL, backup can be scheduled)	Customer owns all Intellectual Property Rights in Customer Data	File versioning Online editing save a file directly to Google Drive integration with current Google products
Policy highlights: https://developers.google.com/storage/docs/terms Termination of services for inactivity for a period exceeding ninety days						
LiveDrive	Backup £4.95/month, £49.95/yr	Any and all files as part of unlimited back up for 1PC	Mac, Windows	Encrypted and stored in multiple places across UK. Up to 30 versions of any file retained in the cloud. Deleted files kept for 30 days.		Access cloud files from other apps using FTP, SFTP and WebDav.
	Briefcase £9.95/month, £99.95/yr	Sync and edit your files up to 2 TB (extra at £4.95 / TB)				
	Pro. Suite £14.95/month £149.95/yr	Sync and edit up to 5 TB (extra at £4.95/TB) for 5PCs with unlimited backup.				
Policy highlights:						
Amazon	Free for 5GB £6 /year for 20GB £16 /year per 50GB up to 1TB (£320)	Designed for AV – if purchased from Amazon then exempt from storage limit – but accepts 'files of any type'.	Web interface so device independent. Desktop folder on Window and Android.	'Permanent delete' removes entirely. 'Deleted' files can be restored. Backup?	Owned data shared via unsecured links.	
Policy highlights: 3.2 Usage restrictions. The Service is offered in the United Kingdom. 5.2 Your right under the Agreement will automatically terminate without notice if you fail to comply with its terms.						

Service	Cost	Formats	OS	Backup	Data Ownership / security	Other features/limitations
SkyDrive	7 GB (free) (Up to 125 GB (paid) 25GB: $2.49 /month 100GB:$4.99/month 1TB $49.99/month	supports viewing of PDF as well as Open Document Format (ODF)	Windows 8, 7, or Vista, Mac OS, X Lion	User is responsible for backing up the data If your service is suspended or canceled, data may permanently get deleted. If data is stored with an expiration date, they may get deleted. Data that is deleted may be irretrievable.	Service Users are the owner and responsible for their data Storage is accessed through https, so it is highly secure	Edit online functionality
Policy highlights: http://windows.microsoft.com/en-gb/windows-live/microsoft-services-agreement						
ADrive	50 GB (free) 50GB to 10TB, Starting at $69.50 100GB to Unlimited Starting at $167	supports viewing of PDF as well as Open Document Format (ODF)	Windows, Mac & Linux	User are responsible for independent backup of Storage Data stored using the ADrive Services, though it grants user a license to use the ADrive back-up software	Service Users are the owner of their data	Edit online functionality File History Recovery Multi-User Accounts Very clear/detailed Ts&Cs
Policy highlights: http://www.adrive.com/terms The ADrive Services are managed from its offices within the State of California and Arizona in the United States of America. ADrive makes no representation that its services are appropriate or available for use in other locations						