



# **Things to do with data: Securing documents and data in the cloud**

Tom Anstey,  
Weatherall Institute of Molecular Medicine,  
University of Oxford

May 2014

# Agenda

What is “the Cloud”?

Threats to data / documents

Protecting data / documents online

Password protection

Introduction to Encryption

Backup

# “The CLOUD”

The “Cloud” can mean a number of things

We are talking about the Internet

Sending data / documents

Storing data / documents

Sharing data / documents

# CLOUD Services



**Dropbox**



**WebLearn**

Collaboration Content Assessment Information Management

**OxFile**



Microsoft®

**SharePoint® 2010**

# Threats

Someone could read something they shouldn't

Could accidentally publish information

Could send something to the wrong person

Documents could be lost

Documents could be changed

Could breach the Data Protection Act

# How do you protect Data online?

It depends!

What is “security”?

# How do you protect Data online?

What are you trying to do?

Is the information personal/confidential?

Who is responsible for it?

Where will the information be stored?

Who will have access?

# How do you protect Data online?

What if it goes to the wrong people?

What if it is made publicly available?

What happens if the document is lost?

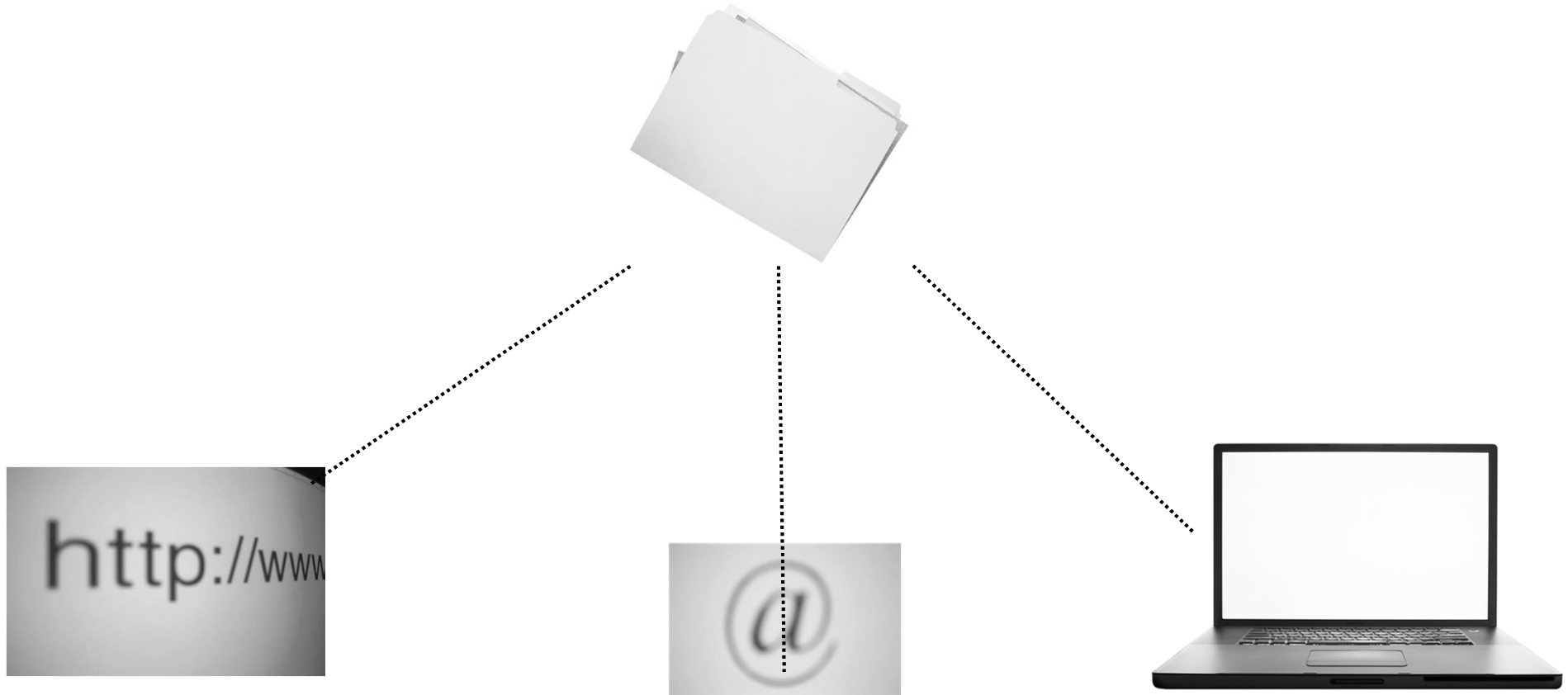
What happens if someone alters it?



# Data security tip 1

THINK FIRST

# WHO HAS ACCESS? For example:



# Who could have access?

You

Anyone who knows your password

Anyone you intentionally share the folder  
with

Anyone you accidentally share the folder  
with?

Anyone with the right link?

# Who could have access?

Not unique to Dropbox

Doesn't mean don't use Dropbox (or other services)

May be appropriate for trusted individuals/small groups

Be aware of the limitations

# Data security tips 2

Secure your own account

Check how access can be controlled

Make sure you send to the right recipients

But make sure (in advance) that they know what is expected of them

Think about preventing other users from sharing

Remove links if appropriate

# Data security tips 3

Where is the data stored?

How is the data stored?

Who might have access to it?

How do you know?

What is the worst case scenario

If it really is sensitive/confidential then  
think again

# Securing your account

Passwords can be guessed, recorded, or phished

Someone could “steal” your session if you don’t log out

# Securing your account

Choose a strong and unique password

Don't share it with anyone

Use machines you trust

Use two-factor authentication

Only use encrypted channels (https)

Make sure it is the right site

Log out when you are done



# Where is the data stored?

Data Protection Act 1998 says.....

*"Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."*

[www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide/principle\\_8.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx)

# Where is the data stored?

## Some advice

All other principles of DPA remain regardless of where the data is stored

Check with [data.protection@admin.ox.ac.uk](mailto:data.protection@admin.ox.ac.uk)

If you are transferring outside the EEA see the ICO's guidance

Check Safe Harbor

There may be other reasons why you don't want to store information externally

# Encryption

It is not essential

Doesn't help if your account is  
compromised

May not prevent administrators having  
access

Useful if someone gains unauthorised  
access...

... but only if the keys remain secure

# How would someone gain access?

Via your account

Via information made publicly available

Breach of security of the service  
(physically or logically)

Rogue administrator

Administrator error

# Private vs Public

- Possibly trust local services more
  - Impact of an exposure probably less
  - Less complicated from DPA point of view
  - Know where the data is stored
- Perhaps greater functionality
  - Easy to use
  - More storage space
  - Possibly offer backup
  - Encryption of data

# Private vs Public

Be aware of the services the University  
and your department/college offer

If they match your needs then use them  
If they don't you may have to look elsewhere

Make sure your needs are known

# What else is there?



- Data security tips 4: treat email like a postcard

Would you send it in Email?

Place Stamp Here

Dear Alice,

Having a great time here in Hawaii! Here is the information you asked for to pass onto the realtor.

Social Security: 931-23-4523  
Birthdate: January 1, 1910  
Credit Card: 2993-2945-6321-4235  
Expiration Date: 08/11/2011  
My Password: BobJR2006

Please let me know if they need anything else to secure the loan.

Thanks,  
Bob

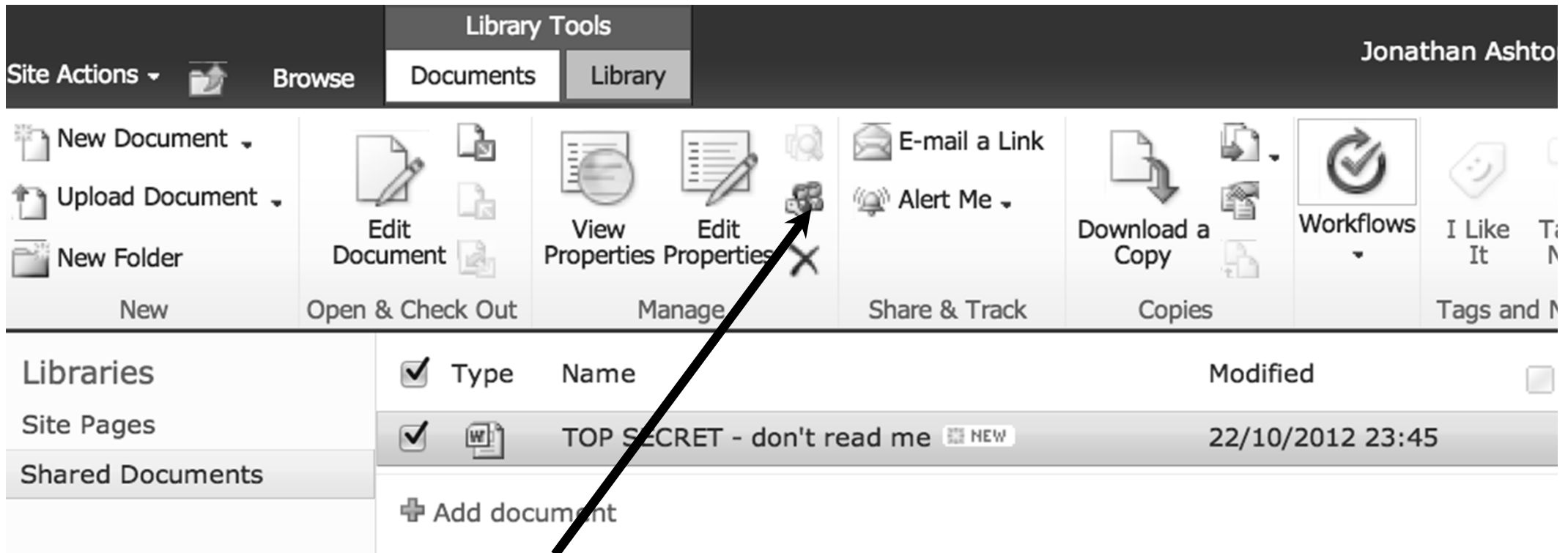
Did you know that an email provides the same level of security as a postcard?

To learn more about this and other security tips, please visit <http://security.ms.cba.ox.ac.uk>

October is CyberSecurity Awareness Month



# What else is there?



The screenshot displays a SharePoint library interface. At the top, there is a navigation bar with 'Site Actions' (a dropdown arrow), 'Browse', and 'Library Tools' (containing 'Documents' and 'Library' tabs). The user's name, 'Jonathan Ashto', is visible in the top right corner. Below the navigation bar, there are several action groups: 'New' (New Document, Upload Document, New Folder), 'Open & Check Out' (Edit Document), 'Manage' (View Properties, Edit Properties, and a crossed-out icon), 'Share & Track' (E-mail a Link, Alert Me), 'Copies' (Download a Copy), 'Workflows', 'I Like It', and 'Tags and M'. Below these actions is a table with columns for 'Libraries', 'Site Pages', 'Shared Documents', 'Type', 'Name', and 'Modified'. A document titled 'TOP SECRET - don't read me' is listed with a 'NEW' badge and a modification date of '22/10/2012 23:45'. An 'Add document' button is located at the bottom of the table. A black arrow points from the 'Add document' button to the 'Edit Properties' icon in the 'Manage' group.

Libraries	Type	Name	Modified
Site Pages	<input checked="" type="checkbox"/>	TOP SECRET - don't read me <span>NEW</span>	22/10/2012 23:45
Shared Documents	<input type="checkbox"/>		

<https://sharepoint.nexus.ox.ac.uk>



# What else is there?

<https://weblearn.ox.ac.uk>

**Worksite Setup**  
Edit Tools | Page Order

**My Workspace**  
Site URL

Name	Role	Remove
Ashton, Jonathan ( jashton )	maintain	<input type="checkbox"/>

Update Participants Cancel Export User List

**Role Descriptions**  
access

Site user: useful for students. By default, this role can read material, take part in assessments and create material within tools such as Forums, Chat and Wiki.

contribute

maintain

Site manager: useful for staff & tutors. By default, this role can modify the site participants and tools, and create and modify content in all areas, e.g., Resources, Forums, and Tasks, Tests and Surveys (assessment).

# What else is there?

## Sharing settings



Link to share (only accessible by collaborators)

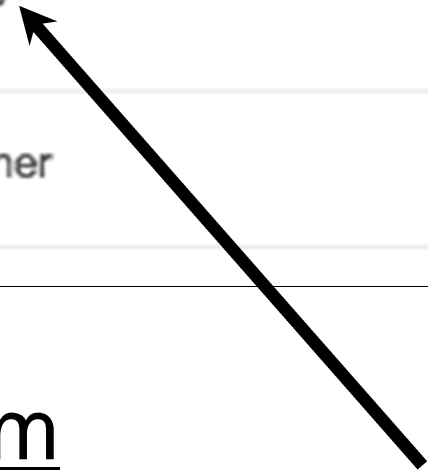
[https://docs.google.com/document/d/1E--oIWm9N\\_Z2gLpK078onbG4N9xygBvkRz2-v](https://docs.google.com/document/d/1E--oIWm9N_Z2gLpK078onbG4N9xygBvkRz2-v)

Share link via:



## Who has access

	Private - Only the people listed below can access	Change...
	Jonathan Ashton (you) jogashton@gmail.c...	Is owner



# Password protection

Perhaps most common way of adding security?

# Password protection

Depends on the implementation

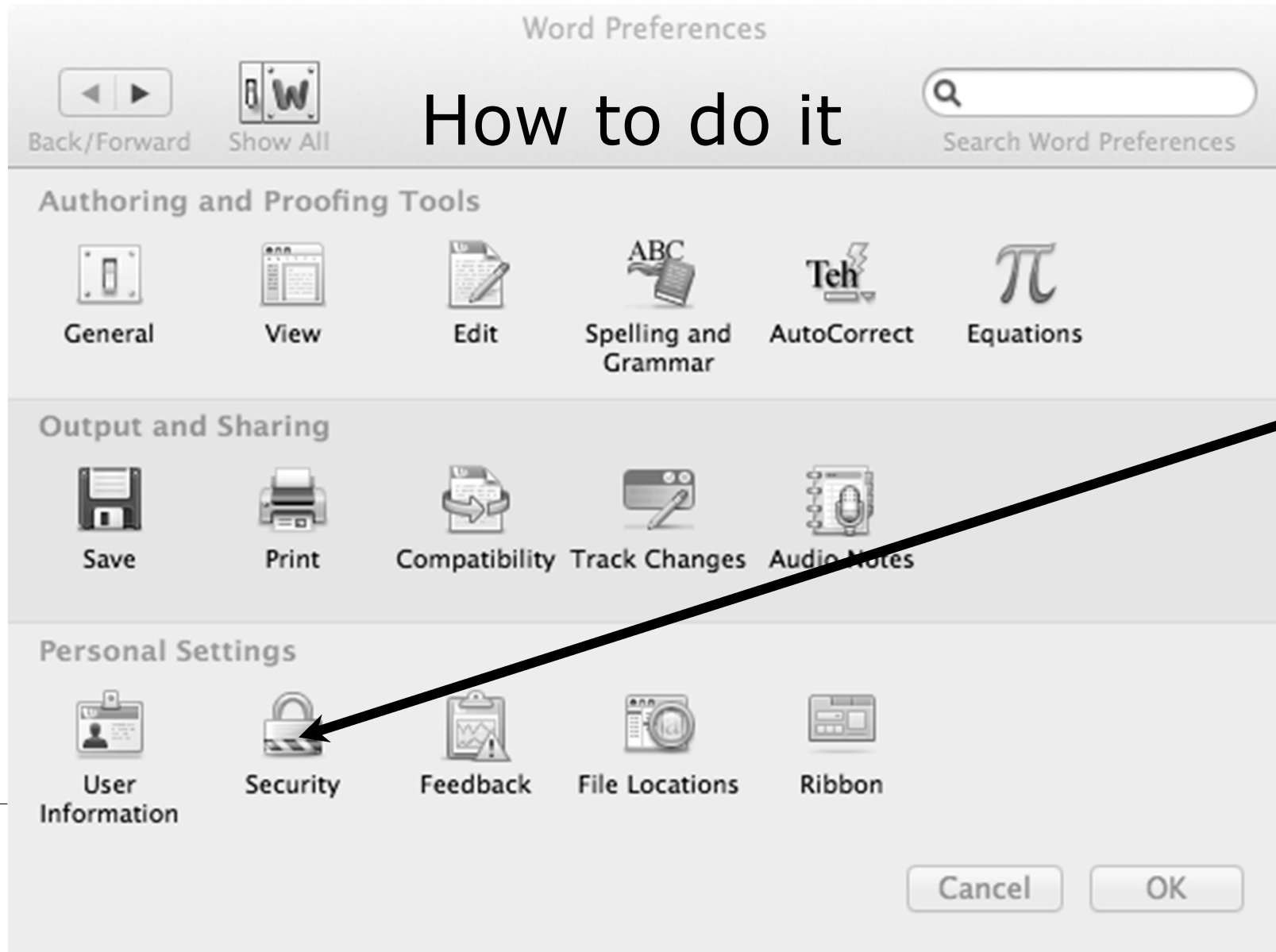
Make sure recognised algorithms are used

Most likely AES

If you are unsure - ask

Depends on the security of the password

# Password protection



# Password protection

Other options

Password protected PDFs

Password protected zip files  
(winzip, 7-zip)

# Password protection

Tips and advice

Password protected documents are (**at best**) only as secure as the password

Use strong passwords

Don't re-use passwords

Use computers you trust

# Password protection

Sharing

In person

Over the phone

**Do not** send with document

If you **have to** send electronically then  
choose another medium (e.g. SMS)



# Encryption - the basics

# Encryption



# Encryption - pros

**If** you trust the encryption key then you know that **only** someone with the decryption key can open the file

Someone intercepting the file alone, won't be able to access

Attacker needs access to the decryption key and password

Can use for email and/or file security

# Encryption - cons

It is more complicated than  
passwords

If you don't understand it can be easy  
to make mistakes

How do you trust people's keys?

# Encryption - further info

<http://gnupg.org>

<http://www.symantec.com/> (PGP  
Desktop)

<https://www.gpgtools.org/>

<http://gpg4win.org/>

# Backup

Remember it is not just about confidentiality

You might be using online services for backup

Or you might be using online services to  
work on files

Either way make sure you know disaster  
recover/back-up plans for the service you are  
using

# Backup

What if the service was  
unavailable?

Don't forget to make sure any  
backups are stored securely

Backup regularly

Make sure you can actually recover data

# Summary

The Internet is very useful for sending, sharing and storing documents!

**You** are responsible for the security of your account

Know the security requirements of the data

Be careful with recipients and security settings



# Summary

Email is inherently insecure

Check where the data is being stored

Check how the data is being stored

Where confidentiality is important use  
extra protection

Make sure you have backups of data  
and that they are secure

# Useful Links

University of Oxford Information Security –

**[www.it.ox.ac.uk/infosec/protectyourself  
/documents/](http://www.it.ox.ac.uk/infosec/protectyourself/documents/)**

Information Security Awareness module

[www.it.ox.ac.uk/infosec/module/](http://www.it.ox.ac.uk/infosec/module/)

Information Commissioners Office [www.ico.gov.uk/](http://www.ico.gov.uk/)

Safe Harbour <http://export.gov/safeharbor/>

Dropbox security overview

[www.dropbox.com/privacy#security](http://www.dropbox.com/privacy#security)

Google Drive Privacy and policies

<http://support.google.com/drive/bin/topic.py?hl=en&topic=2428743&parent=2375072&ctx=topic>