

# Suggested data handling

When handling people's sensitive data it's important to make sure that you are taking reasonable precautions to keep their data safe and secure.

## Digital Information

When storing digital information on a computer you should ensure that the data is reasonably secure. Whole disk encryption is the best way to ensure that the information is kept secure whilst it's "at rest" on your machine. You should also maintain some form of up to date antivirus and firewall on your machine.

All information on a hard drive should be wiped before disposing of the machine.

## In "the Cloud"

For information kept using an online service, such as Google Docs or Eventbrite, you should make sure that you have a password which is adequately secure. If additional security can be put in place, for example 2 factor auth using a token or your phone, then you should enable it and use it.

*Note: In EU countries you will need to ensure that data held outside the EU is held with an adequate level of protection. If it's being held in the US then make sure the provider is listed at <http://safeharbor.export.gov/list.aspx>.*

## Physical Files

Data in a physical form, such as files, should be kept in a locked cabinet and not stored in a public area. Only those who need access to the information held should have access to a key for the cabinet.