1. The best place to store your current paper-based data while you are working on it is: (choose one answer only)
   a) on your desk
   b) in an unlocked drawer
   c) in a locked filing cabinet
   d) in a vault

2. Backing-up your data (choose all possible answers)
   a) protects against data loss or corruption
   b) preserves it forever
   c) should be done regularly
   d) is the sole responsibility of your institution

3. How often should you copy or migrate your digital data onto new tape media? (choose one answer only)
   a) every day
   b) every month
   c) every year
   d) every 2-5 years
   e) every 20 years

4. What should you do with paper-based data to ensure the longevity of the information? (choose all possible answers)
   a) store it in a temperature/humidity-controlled environment
   b) store it in direct sunlight
   c) convert it to PDF/A format and store in a location fit for purpose
   d) store it in your attic

5. How should you ensure the security of personal information in a dataset? (choose all possible answers)
   a) by anonymising/reducing the precision of the data
   b) storing names/addresses separately from the other data
   c) encrypting data containing personal information
   d) requiring data users to sign the Official Secrets Act

6. Encrypting files on your mobile storage device ensures that your digital data are: (choose one answer only)
   a) open for anyone to see
   b) protected and only those with the encryption key can view them.
   c) completely deleted
   d) converted into a new format

7. What ways would be suitable for transferring transcribed research data to a colleague? (choose all possible answers)
   a) via an unencrypted email attachment
   b) using Dropbox without encryption
   c) using Dropbox with encryption
   d) hand it in person to the recipient on a USB stick

8. How can you securely destroy data on a personal computer hard drive? (choose all possible answers)
   a) delete files and reformat the hard drive
   b) remove and shred the hard drive
   c) delete files and take the computer to the dump
   d) overwrite files using secure deletion software

9. How can you securely destroy data on a CD/DVD disc? (choose one answer only)
   a) put it through a CD shredder and throw it away
   b) break it in half and throw it away
   c) put it in the plastic recycling bin
   d) put it in the dishwasher on a hot cycle
   e) overwrite files on the disc using proprietary software
1. The best place to store your paper-based data while you are working on it is:
   a) on your desk
      Incorrect. This is not the ideal option if you are in a shared office. It may be less problematic if you are in a single, lockable office and the only person with the key.
   b) in an unlocked drawer
      Incorrect. Again this is not the ideal option if you are in a shared office. It may be less problematic if you are in a single, lockable office and the only person with the key.
   c) in a locked filing cabinet
      Correct. This is the ideal solution
   d) in a vault
      Correct. This would be a good, but not very realistic option for most people.

2. Backing up your data
   a) protects against data loss or corruption
      Correct.
   b) preserves it forever
      Incorrect.
   c) should be done regularly
      Correct.
   d) is the sole responsibility of your institution
      Incorrect. Your institution may back up data on your networked drives but it is not the sole responsibility of the institution, you should also take responsibility for backing up your data.

3. How often should you copy or migrate your digital data onto new tape media?
   a) every day
      Incorrect. Not necessary
   b) every month
      Incorrect. Not necessary
   c) every year
      Incorrect. Not necessary
   d) every 2-5 years
      Correct. This is recommended, e.g. migrate to new media as optical and magnetic media are subject to degradation
   e) every 20 years
      Incorrect. Not often enough

4. What should you do with paper-based data to ensure the longevity of the information?
   a) store it in a temperature/humidity-controlled environment
      Correct.
   b) store it in direct sunlight
      Incorrect.
   c) convert it to PDF/A format and store in a location fit for purpose
      Correct. This is a long-lasting digital format.
   d) store it in your attic
      Incorrect.

5. How should you ensure the security of personal information in a dataset?
   a) by anonymising/reducing the precision of the data
      Correct.
   b) storing names/addresses separately from the other data
      Correct.
   c) encrypting data containing personal information
      Correct.
   d) requiring data users to sign the Official Secrets Act
      Incorrect. Not necessary!

6. Encrypting files on your mobile storage device ensures that your digital data are:
   a) open for anyone to see
      Incorrect.
   b) protected and only those with the encryption key can view them
      Correct.
   c) completely deleted
      Incorrect.
   d) converted into a new format
      Incorrect.

7. What ways would be suitable for transferring transcribed research data to a colleague?
   a) via an unencrypted email attachment
      Incorrect. This is insecure.
   b) using Dropbox without encryption
      Incorrect. This is insecure.
   c) using Dropbox with encryption
      Correct.
   d) hand it in person to the recipient on a USB stick
      Correct. This is fine, but make sure they look after it!
QUIZ ANSWERS: DATA STORAGE AND SECURITY

8. How can you securely destroy data on a personal computer hard drive?
   a) delete files and reformat the hard drive
      Incorrect. This is insecure.
   b) remove and shred the hard drive
      Correct.
   c) delete files and take the computer to the dump
      Incorrect. This is insecure.
   d) overwrite files using secure deletion software

9. How can you securely destroy data on a CD/DVD disc?
   a) put it through a CD shredder and throw it away
      Correct.
   b) break it in half and throw it away
      Incorrect. This is not failsafe.
   c) put it in the plastic recycling bin
      Incorrect. This is not failsafe.
   d) put it in the dishwasher on a hot cycle
      Incorrect.
   e) overwrite files on the disc using proprietary software
      Incorrect. This is not failsafe.