Answers to Exercise 6.1

**Scenario 1**. Unshredded and unanonymized printed data transcripts from a research project exploring abusive relationships are found on the street in a clear plastic rubbish bag. It was too time-consuming to shred the large pile of documents with a basic office shredder, so the research team decided to just throw them into the recycling bin.

***Preventative measure***: Ensure that the data are securely disposed of via an institutional shredder (DIN 3 minimum) or use an approved bulk shredding service available that can carry out the task. Personal data or confidential information should not be placed into the recycling bin.

**Scenario 2**. A senior lecturer stores personal and confidential data on the hard drive of her university computer. She is given a new computer by her department, while the old one is given to research students to use in their office. The students are able to access both the personal, confidential and research data on the computer.

***Preventative measure***: Ensuring the data were encrypted in the first instance could have helped prevent unauthorized access to the personal and confidential data. It is important to not assume that IT services will clean or reformat the hard drive before passing on the computer. Always securely delete the data files stored on a hard drive when disposing of a computer. Only ‘scrubbing’ or physical destruction will sufficiently delete them from the machine.

**Scenario 3**. A researcher has a laptop stolen whilst away on a conference trip. Vital research data was kept on the hard drive and was not backed up anywhere else.

***Preventative measure***: Always keep a backup of data. When travelling you should remove all unnecessary data from the laptop and create a backup on an appropriate device and onto another hard-drive back at home/the office. If the data contains personal or confidential information, then it should be encrypted (including the backup). Under the GDPR you have a legal obligation to protect personal data relating to living people, such as, real names and addresses, so it needs to be stored securely, especially when travelling.

**Scenario 4**. A researcher sends a USB memory stick with audio recordings for transcription in the post. The researcher writes the wrong address on the package and the USB memory stick gets lost in the post.

***Preventative measure***: Address packages carefully and send via a trackable courier service. In the UK, the Royal Mail offer special delivery services. Always make duplicate copies before sending and ensure the data are encrypted.

**Scenario 5**. Digital audio files are emailed to a transcriber who saves them to his computer desktop and also stores them in his email once received. The transcriber fails to delete the files from his email and from his computer once the transcription is completed and returned to the researcher. He later sells his computer on eBay.

***Preventative measure***: Ask transcribers to sign an agreement to destroy their copies of the data once they have been returned and verify after transcription that this has indeed been done. It is best not to email files that you do not want to remain on other people’s computer systems. You should encrypt the files before sending them via secure transmission.

**Scenario 6**. A researcher works in a shared office with four other researchers working on other projects. Whilst working on his project the researcher leaves paper copies of the signed consent forms loose on the desk. The other researchers have the opportunity to read through these confidential documents.

***Preventative measure***: Always keep confidential documentation and data in a locked filing cabinet. Do not keep the key in the lock; store the key in a secure place.

**Scenario 7**. A transcriber tells her friends and family about the ‘interesting interview’ that she is transcribing, giving details about the name and place of work of the interview participant.

***Preventative measure***: Ask transcribers to sign non-disclosure agreements, preventing them from divulging confidential information and remind them of the nature of information sent to them and their responsibility to keep that information confidential.

**Scenario 8**. A fire at the university destroys a research office and all the paper copies of an important research collection that a researcher was preparing for archiving.

***Preventative measure***: Always keep backup copies of important data in an offsite location. With important paper documents, these can be scanned encrypted and kept digitally.

**Scenario 9**. Unanonymized data are inadvertently published on a project’s website.

***Preventative measure***: Unanonymized data must be kept safely and only accessed by those permitted to use it. Always double check that appropriate anonymization has been carried out before data are published. Methods such as statistical disclosure control can help here.

**Scenario 10**. A researcher encrypts his data folder, then forgets his password and can no longer access his data.

***Preventative measure***: The researcher could also have kept a paper copy of the password away from the computer and the data folder.