Chapter 1

What is a Bookkeeper?

In this chapter we will be looking at the role of a bookkeeper and how it differs and compliments the role of an accountant. We will look at the need to keep skills and knowledge up to date. We will look at why it is necessary to keep information confidential and how this can be done. We will look how and why we need to act ethically as a bookkeeper.

All businesses need to keep a record of their financial transactions. Firstly it is a requirement of Her Majesty's Revenue and Customs (HMRC). Businesses are required to keep accurate details of their income and expenditure. There are hefty fines if you don't.

However, apart from the legal requirements, a business owner will want to know the income and expenditure of the business, both on a day-to-day basis and in the long term. If the owner doesn't keep records then the business may be spending more money than it receives which could result in ruin for the owner. Even if the owner knows that there is more income than expenditure, he or she will want to know the financial position of a business so that they, or the managers, can make informed decisions that will improve or expand the business.

Unless you work for a limited company (Ltd)[1] it is quite acceptable to keep these records in any way the owner wishes as long as it is clear how much money is coming into the business and how much is going out. However, if this is not done in an organised way then it will be time consuming to gather all the information together when it is needed.

Over the many years that financial records have been kept, cost effective and efficient systems have emerged. It is these systems that we will be looking at in this book.

Before the time of computers, businesses used to keep their financial records in **books**. There would be a different book for each different type of transaction. Sales would be kept in one book, while purchases would be kept in another. A record of the business's cash position would be kept in a cash book. We will look at many of the different types of books later in this study manual. So it is logical that someone who looked after these books was called a **bookkeeper**. This name still continues even though the 'books' are now often stored on a computer.

Many traders are skilled at whatever goods or services they offer. But running a business is time consuming. Therefore, all but the smallest businesses will employ someone to keep the

[1] Limited company accounts are dealt with in other AAT courses

books up to date, while the trader will get on with the business of selling his or her goods and services.

Bookkeeper

A bookkeeper is someone who records all the financial transactions of a business. The most important actions of any business is buying and selling. The bookkeeper will record the details of all day to day sales and purchases in **day books**. They are called day books because daily transactions are recorded here. There will be a day book for sales and another for purchases. Obviously sales and purchases will involve the transfer of money, so the bookkeeper will also record the movement in and out of the business in a **cash book**. All books which record these transactions as they happen are called **books of prime entry**. In this case ‘prime’ means ‘first’ so these books are where the transactions are first recorded.

The bookkeeper is unlikely to be present at every transaction, so he or she will record transactions in the books of prime entry from **prime documents**. Typically a prime document is a receipt or an invoice, although we shall see later that other documents may fall into this category.

It is usually the responsibility of the bookkeeper to check the accuracy of these documents. Inaccurate documents or inaccurate recording of these documents can waste time and money and could result in the business losing money. We will look at how to check for errors in documents later in this study manual.

Larger businesses may employ several bookkeepers to deal with different types of transactions. For example there may be a bookkeeper who deals only with sales, dealing with customer invoices and statements. This is often referred to as the receivables (or sales) ledger. Another bookkeeper may deal with only purchases and suppliers, known as the payables (or purchases) ledger. (The people you buy from are known as **suppliers** and the people you sell to are **customers**). They will be responsible for supplier invoices and payments. Another bookkeeper may be the cashier who is responsible for recording the money received and money paid by the business.

Even though there are rules on how to present the financial information for limited companies (Ltd), a bookkeeper will still have to record the day-to-day transactions. These records can then be used by the accountant to present the information in the required format. The financial information provided by the accountant will tend to be for the business as a whole, whereas the bookkeeper will deal with the individual transactions.

Bookkeepers may also be responsible for chasing customers for payment or preparing documentation (including cheques) for paying suppliers.

CHAPTER 1
What is a Bookkeeper?

Accountant

We mentioned 'accountant' in the previous section. Many people, including business managers, confuse the different roles. Both bookkeepers and accountants deal with financial records, but an accountant will deal with the presentation and interpretation of the figures.

The accountant may be responsible for advising on, and calculating taxation. Individuals and companies are all liable to taxation. Unlike employees, people with businesses are responsible for their own tax issues and the payment of amounts due. Accountants may calculate how much tax is due and complete the forms which are to be presented to **Her Majesty's Revenue and Customs** (HMRC). HMRC is the government department which deals with taxation in the UK.

An accountant may also be responsible for interpreting financial information. He or she may have to make decisions on future events in the business based on the business's past record. This may involve giving advice on the selling prices of goods, if it would be financially viable to go ahead with a new product, or whether to buy new machinery for the factory.

Whatever the accountant may be required to do, he or she will rely on the accurate information provided by the bookkeeper. If the bookkeeper gets it wrong then the accountant will also provide false information. The result could be disastrous for the business. The bookkeeper, therefore, has a responsibility to ensure that the information they provide is accurate, up to date and complete. A bookkeeper should never enter any transaction into the business's books unless they are sure it is free from errors, and nothing is missing. It should also be entered into the books in a timely manner. It's no use to the business if the transactions are recorded late. Anything the bookkeeper is not sure about must be referred to the manager or accountant and must not be entered into the books until the bookkeeper is confident it is correct.

In practice the roles of the bookkeeper and accountant are not as clearly defined as above, but this is a guide to the traditional duties of each.

Confidentiality

A bookkeeper will have access to a lot of confidential information. Confidential information is a valuable asset to any business. A business may have a competitive edge if it has information that its competitors do not. For example, you may have a special recipe or process for your goods, or you might be planning a sales promotion to gain extra customers. In both cases, if your competitors found out about this, it could adversely affect your own business.

There have been several recent news reports where the names and addresses of customers and suppliers have been stolen due to inadequate confidentiality systems. Not only is this a breach of the law (see below), but it also damages the reputation of the business and can lead to losing customers or suppliers.

The person who is responsible for the data security breach also faces problems professionally. It may breach the employment contract and it may lead to a loss of trust by managers or owners of a business. The personal reputation of the employee could be permanently damaged.

There are two main types of confidential information.

1. Commercial information

This information is information about the business and its activities. Bookkeepers must ensure that they don't disclose details of the business's current activities or planned future activities which may give a competitor an advantage. It may include manufacturing processes and methods, business plans, financial data, computer programs or recipes. A bookkeeper is likely to come into contact with the business's financial data on a daily basis, so safeguards are needed to ensure that this data doesn't get into the wrong hands, even accidentally. A bookkeeper should not discuss the business's financial activities with anyone not authorised to know it. This includes not discussing the details at home or with friends. There are no laws which prevent the disclosure of this type of information, but there would be serious repercussions with the business itself and any professional body (such as the AAT).

2. Personal information

Businesses have a duty to keep personal information secret. If it is not kept secret personal details may find their way into the public domain which individuals don't always want and in some cases can be detrimental to the individual involved. Personal data may be held about customers, suppliers and employees and is protected by law. The **General Data Protection Regulations (GDPR)** was passed by the European Union (EU) and came into effect in 2018. It came into British law under the Data Protection Act 2018. Since Brexit the GDPR and the Data Protection Act have been updated to accommodate domestic areas of law, and is now known as the UK-GDPR. However, the core rules remain the same.

The Data Protection Act 2018 regulates how personal information is used and prevents misuse of personal details.

Data means any information which is held either on a computer or manually.

Personal data means data which relate to a living individual. It is not personal data if, for example, you have records of the number of customers visiting your shop, but it is personal data if those customers can be identified, even if only by a reference number.

Data subject means an individual who is the subject of personal data

Data controller means, a person or persons who determine the purposes for which and the manner in which any personal data are processed

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
The Data Protection Principles are:

1. Data should be used fairly, lawfully and transparently.

2. Data should be used for specified, explicit purposes.

3. Data should be used in a way that is adequate, relevant and limited to only what is necessary.

4. Data should be accurate and, where necessary, kept up to date.

5. Data should be kept for no longer than is necessary.

6. Data should be handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Under the Act, the individual has the right to:

- be informed about how the data is being used.
- access personal data.
- have incorrect data updated.
- have data erased.
- stop or restrict the processing of the data.
- be allowed to get and reuse the data for different services.
- object to how the data is processed in certain circumstances.

The Act gives data subjects rights to access personal data about themselves which is held in either computerised or manual form. This extends to a description of the data held, the purposes for which it is processed and to whom the data may be disclosed

If the data subject believes that data recorded about them are inaccurate the person may apply to the court, for an order which may require that the inaccurate data, and any expression of opinion based on it, is rectified, blocked, erased or destroyed.

The Data Protection Act 2018 requires every data controller who is processing personal data to register with the Information Commissioner's Office and pay a fee unless they are exempt. Failure to notify is a criminal offence. However, data controllers who only process personal data for staff administration are exempt from notifying.

Companies may set out their own policies on confidentiality. For example, they may require that computer screens are switched off if the user is not at their workstation, or they may restrict access to certain offices which contain sensitive information. Passwords may be used to restrict access to some (or all) electronic data.

LEARNING POINT

For the AAT assessment, you won’t need to know the precise content of the regulations, but you will need to know that these areas are covered by legal requirements. Detailed knowledge of the content of the GDPR is not required.

Data Security

Data security is about keeping data safe. Data may be kept either as a soft copy or as a hard copy. A soft copy is an electronic copy of the data which can only be viewed through an electronic medium. Examples of soft copy data are files viewed on a computer screen or attachments to an email. When these files are printed, they become hard copies.

Hard copy data should be kept in a locked storage device such as a filing cabinet. If the hard copy is being used and the user needs to be away from the desk then it may be stored in a locked drawer.

You should try to ensure that the documents cannot be overseen by others. Keep the documents face down on the table until you need them and ensure you are not in a position where the documents can be read easily by others. This is particularly important if the documents are being used in a public area such as in reception. There have been recent cases where confidential government papers have been read by high-definition cameras used by journalists where the paper is being held in the hand rather than carried in a briefcase or folder.

As many businesses rely heavily on computer systems, loss or theft of this data can lead to disastrous consequences. A malicious email can compromise the data stored on a computer or computer storage system.

Data kept on a computer may include names and addresses of staff, suppliers and customers. It may keep the financial information of the business. It may keep wages and salaries details. All kinds of confidential data is stored on the computer and loss of this data can seriously affect the organisation's ability to do business as well as leading the business into legal problems as we have seen in the GDPR regulations. The maximum fine for the most serious cases of breach of the GDPR is €17.5 million or 4% of the business's entire global turnover, whichever is greater.

Data may be:

- Lost or damaged during a system 'crash'. This is where the computer stops functioning properly. It is particularly serious where the hard drive or storage system fails. The data could be lost forever.

- Corrupted as a result of faulty disks, disk drives or power failures. Corrupted data is data that is changed unintentionally due to errors during writing, reading, storage or transmission.

- Lost as a result of accidental deleting or overwriting files

- Lost or corrupted due to computer viruses. A computer virus is a piece of code or program which is loaded onto the computer without the user's knowledge (often through an email attachment). Virus programs can alter or destroy data on a storage system without the user being aware that the program is running.

- Hacked into by unauthorised users. A hacker is someone who is able to break codes and bypass passwords to gain unauthorised access to files stored on a computer system.

- Destroyed by fire or flood or other natural disasters.

- Altered or deleted by employees with a grudge or wishing to make money out of illegally selling or altering data.

- Phishing. A phishing email is designed to look like an email from a legitimate source. Typically, they appear to come from banks, the government or a major company. They deliver a sense of urgency or fear to persuade the user to give up sensitive data. If you receive an unsolicited email, be sure to check it's from who you think it's from before doing what the email asks.

Data can be kept secure by taking security measures:

- Using passwords. This is a string of characters which allow access to a computer system or file. This is the first line of defence against unauthorised access to a computer system or file. Some web sites also use two-step authentication. This is where another layer of protection is added to the password. The second layer may be a Personal Identification Number (PIN), or it may be an SMS message sent to your phone. It may even be a person's fingerprint, retina pattern or facial recognition.

- Taking regular backups. A backup is a copy of a file in case the original is lost or destroyed. Backups can be kept in the '**cloud**'. This is where data is stored on the internet rather than on the computer, so files can still be retrieved if the computer storage system is stolen or destroyed. Files can also be accessed from any device anywhere in the world that has internet access (remote access). Some data may have restricted access, where only certain staff are allowed to view or update the files. This restriction often takes the form of a password. The password ensures authentication is required to access these files.

- Archiving data. This is a process of moving data that is no longer actively used but must be kept for operational or legal reasons, to a separate storage device. This reduces the volume of data that must be backed up at regular intervals.

- Running anti-virus software. This is a program which is designed to detect and destroy virus programs.

- Using a firewall. A firewall monitors incoming data (called 'traffic') from other networks (such as the internet) and blocks suspicious traffic such as viruses and hackers.

- Using security software and passwords when accessing business data remotely from anywhere in the world that has an internet connection. This can be used where there is access to the data from the business premises as well as remote access (hybrid working).

- Always logging off. Logging off means that the user will end their session and anyone else who needs to access the computer will need a password to do so. This is usually quicker than shutting down the computer and so is more useful during the course of a business day. Some businesses require that you log off even for short periods away from the computer, such as bathroom breaks. Sometimes a program will automatically log off after a specific length of time of inactivity.

- Using screensavers. A screensaver is a computer program that removes the display after a designated time, often replacing it with moving images or patterns. The original use of a screensaver was to prevent the monitor screen from damage by showing the same image for long periods. While most modern monitors are no longer susceptible to this problem, screensavers are still used to hide data shown on the screen when the computer is not in use. Often the user will need to input a password to regain access to the data on screen.

- Write-protecting files. This means that the file can be read but cannot be altered without the correct password. This can be set up for the whole file or (in the case of spreadsheets) part of the file.

- Encryption. This is where the data is scrambled so that it cannot be read by anyone intercepting it. The sender has a program which scrambles the data and the receiver has a program which unscrambles (decrypts) the data. It's not used by all businesses as it is slower than 'plain text' (unencrypted data) and it is not free for businesses to set up and use.

- Ensuring that your screen cannot be overlooked easily and not sharing computers or laptops with others.

- Not discussing confidential information where others may hear.

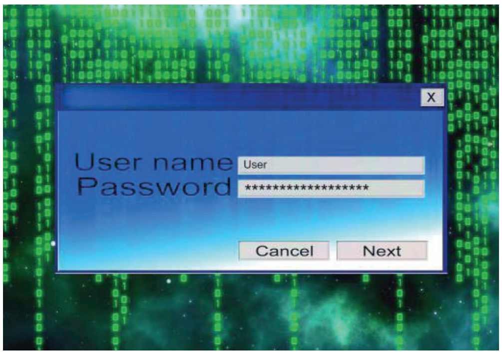
- Setting cookies and privacy settings. A cookie is a small file that web servers send to browsers. These cookies are then sent back to the server in order to remember your preferences and habits. They can be good as they will suggest related searches and suggest related products you can buy. The problem with some cookies is that they collect data which can be passed on third parties. You can set your cookie preferences to reduce the chance of sensitive information being collected and sold to others.

- Ensuring you share information only with those who are authorised to access this information.

- Checking the correct recipient before sending information.

Passwords

A password is a word or string of characters used for user authentication. A bookkeeper may have many passwords to access different systems and processes on the computer. There may be different levels of password. For example there may be a password to access the computer system, another to access the program such as the accounting program and a third to access the actual documents.



Passwords must be kept secret and should be changed regularly. Most organisations specify a password policy that sets requirements for the composition and usage of passwords, and how often they should be changed. There may be a requirement for a minimum number of characters, or there may be a requirement for it to have a mixture of letters, numbers and symbols.

The easier a password is for the owner to remember generally means it will be easier for an attacker to guess. However, if the password is difficult to remember it may actually reduce security because the user might need to write down the password, or they may use the same password over and over. Passwords which are notoriously easy to guess are

- The name of family members
- The name of family pets
- Favourite sports teams
- The word 'password'

A compromise must be made between making the password memorable and ensuring that it can't be guessed.

Some systems have a double line of security. A password will be required to access the system and then a memorable word must be used before full access can be gained.

Money Laundering Regulations

Money laundering is an illegal process whereby large amounts of money, generated by criminal activity, appears to have come from a legal source. The money could have come from activities such as drug trafficking or terrorist funding and is ‘dirty’ money. Money laundering attempts to make the money look ‘clean’.

Bookkeeping is an accountancy service and so it is included in what is known as ‘the regulated sector’. The **Proceeds of Crime Act 2002** and the **Terrorism Act 2000** require that business and individuals in the regulated sector report any suspicion that a client, supplier, colleague, or employer is involved in money laundering activities. Failure to disclose this information could result in a maximum penalty of 5 years’ imprisonment and/or an unlimited fine. They may also face disciplinary proceedings by their professional accounting body (such as the AAT). Reporting this information is called a **protected disclosure** which means that the individual is protected against allegations of breach of confidentiality.

Where an individual or business offers bookkeeping services to the public, they must register for anti-money laundering supervision. They can do this through their professional body or with Her Majesty’s Revenue and Customs (HMRC). Failure to do so is a criminal offence.

Where money laundering is suspected, the individual **must** inform the National Crime Agency (NCA) in a Suspicious Activity Report (SAR). Larger businesses will appoint a Money Laundering Reporting Officer (MLRO). Any suspicion of money laundering will then be reported to the MLRO in an internal report. The MLRO will then decide if the activity needs to be reported to the NCA.

There is an additional offence of ‘tipping off’. Where an individual knows, or suspects the MLRO or the NCA have been informed of a suspicious activity, they must not tell the client that a report has been filed. The individual does not have to intend to inform the client for an offence to have been committed. Accidental or unintended tipping off is equally liable to prosecution. The maximum penalty for tipping off is 5 years imprisonment and/or an unlimited fine. However, an individual is entitled to speak with their clients in general terms about money laundering issues.

Ethical Behaviour

Ethical behaviour is about doing the right thing at the right time. All bookkeepers are expected to act in the public interest and to promote high ethical and technical standards.

Bookkeepers registered with the AAT have five fundamental ethical principles to follow as a guide to ethical behaviour.

- **Integrity**

  This is about being honest, truthful, straightforward and having strong moral principles.

- **Objectivity**

  This is about not being influenced by personal feelings or opinions in considering or representing the facts. It is also about representing the facts as they are, without the undue influence of others.

- **Professional Competence and Due Care**

  This is about maintaining professional knowledge and skill and keeping up with new developments, legislation and techniques to ensure that the client or employer receives the best possible service. It is also about not acting recklessly and without due consideration of the facts. Sufficient time should be given to each task in order to complete it competently.

- **Confidentiality**

  This is about keeping information acquired as a result of business activities, secret. Such information should not be used for personal gain, or disclosed to anyone else without explicit permission to disclose it, or where there is a legal requirement to disclose it.

- **Professional Behaviour**

  This is about acting in a professional way (both in the workplace and outside), being a law-abiding citizen, and not bringing the accountancy profession into disrepute.

There is no set of specific rules detailing what should happen in a given situation, but instead these guidelines should be used so the individual can come to the right decision on what course of action to take.

Chapter Summary

- A bookkeeper records the financial transactions of a business in day books, while an accountant presents and interprets this data.
- A bookkeeper records transactions in day books and a cash book (which are books of prime entry) from prime documents.
- Bookkeepers must ensure the data they record is accurate and is recorded in a timely manner.
- Bookkeepers must be aware of confidentiality and make every effort to keep sensitive information secret.
- Data must be kept securely. The bookkeeper must know the techniques to reduce the chance of data loss.
- Bookkeepers have a legal responsibility to report suspicions of money laundering.
- Bookkeepers, as well as all other financial professionals, must act ethically.

Practice Questions

Chapter 1

1.1

State whether the following statements are true or false.

Statement	True	False
A bookkeeper will prepare the financial statements of a limited company (Ltd)		
A bookkeeper is responsible for checking the accuracy of the figures on supplier invoices		
A bookkeeper may be responsible for chasing payment from customers		
A bookkeeper may be responsible for authorising the purchase of a new photocopier.		

1.2

State whether the following statements are true or false.

Statement	True	False
Personal information kept by businesses on their employees is protected by law		
In all cases, personal information may only be processed by a business if the individual gives written consent		
Once consent is given, personal data may be kept indefinitely		
Disclosing commercial information is prevented by the General Data Protection Regulation		

1.3

You are working with some confidential hard copy documents. Your manager has requested a meeting to discuss another job he wants you to do tomorrow. You will be away from your desk for about half an hour. What should you do with the documents on your desk?

Select the most suitable action:

Action	√
Turn the documents over so that no one passing your desk can see them	
Give them to a colleague for safe keeping	
Put them in your drawer and lock it	
Hide the documents under some other papers	

1.4

State whether the following statements are true or false.

Statement	True	False
All businesses must appoint a Money Laundering Reporting Officer.		
Only individuals working in the regulated sector have a duty to report suspicions of money laundering.		
All businesses and individuals which offer bookkeeping to the public must register for anti-money laundering support.		
An individual must not discuss any general money laundering issues with their client.		

1.5

What are the five fundamental ethical principles suggested by the AAT?

1 ______________________________

2 ______________________________

3 ______________________________

4 ______________________________

5 ______________________________