

Handling confidential information

- Do you handle confidential information?

- Do you know what makes information confidential?

- All team leaders need to recognise confidential information and treat it with care.

This session will help you to recognise the different types of information that team leaders will use. You will look at the reasons why some information is confidential and what your role is in maintaining and ensuring confidentiality. You will also learn about some of the law on confidentiality.

What is confidential information?

Confidential means that only certain people have permission to know about particular things. For example medical records are normally only seen by health professionals and patients themselves. In your day-to-day work as a team leader you will handle different types of information, which will be on paper, electronic and spoken. Some of this may be confidential

Handling confidential information



However, much of this information will not be confidential. It is your responsibility to know what is confidential and what is not confidential. Generally speaking, information will be confidential if it is about:

- ❖ another employee,
- ❖ a client or customer, or
- ❖ it is sensitive information about the organisation.

Sensitive information on the organisation may include information about its finances, new projects, reorganisations and mergers. Any information that would give a competitor an advantage can be considered confidential.

A useful rule for you to follow, if you aren't certain, is to keep the information confidential until you have checked. Team leaders should use their common sense regarding matters of confidentiality. For example, if someone tells you something about their private life or of a personal nature it is respectful not to broadcast this to others. Team leaders should encourage team members and others at work not to gossip and to respect other people's privacy.

Useful people in organisations to check whether information is confidential will include your:

- ❖ Personnel department
- ❖ Administration department
- ❖ Line manager
- ❖ Legal department

Exercise

Think about all the different types of information that you handle at work. Using a large sheet of paper with "information" written in the centre write down around it as many types or sources of information as you can. Your list could include:

- ❖ Application forms
- ❖ Personal details on clients
- ❖ Memos
- ❖ Staff CVs
- ❖ Personal data
- ❖ Emails
- ❖ Minutes of meetings
- ❖ Briefing sheets
- ❖ Newsletters or bulletins
- ❖ Letters

When you have completed your spider diagram (which is what this kind of diagram is called):

- ❖ using a coloured pen, circle all those types of information that you know are confidential;
- ❖ give the reason why this information is confidential;
- ❖ make a list of those items which may be confidential depending on what they are about. (For example not all memos are confidential but a memo about a complaint against a member of staff would be.)

Looking at the types of information that are confidential, do they have anything in common? You will find that:

- ❖ all private information about employees is confidential;
- ❖ all personnel documentation is confidential (discipline cases, for example);
- ❖ all personal data on customers is confidential; and
- ❖ sensitive information on the organisation is confidential.

Have you identified any others?

How is confidentiality regulated?

There are a number of regulations to help you understand what is confidential and to ensure that you and your team members keep to the rules on confidentiality. The three main types of regulations controlling matters of confidentiality are listed below, with some examples:

Regulation	Examples
Organisation policies	❖ Employment policies, Discipline procedure, Policy on Emails
Legislation (the law)	❖ Data Protection Act 1998, European Directive on Data Protection, Human Rights Act 2000 and aspects of civil law
Professional codes of conduct	Examples: <ul style="list-style-type: none">❖ Chartered Institute of Personnel Development (Personnel)❖ British Association of Counselling (Counsellors)❖ Law Society (Solicitors)❖ Chartered Institute of Management Accountants (Accountants)

Exercise

To help you understand these three main types of regulation on confidentiality you will need to carry out some research:

1. Find out what policies and procedures your organisation has concerning confidentiality (you may need to ask your line manager or your personnel department).
2. You can also ask what the organisation's rules and procedures are about confidentiality in relation to the Data Protection Act or the Human Rights Act.
3. Find out if there are any employees that are covered by a professional code of conduct for matters of confidentiality. Ask them how they are required to behave.

The Data Protection and Human Rights Acts

Both the Data Protection Act and the Human Rights Act are complex pieces of legislation. The **Data Protection Act** was originally passed in 1984 but was updated in 1998 to include manual (non-computer) records). It is the key piece of legislation on confidentiality. The most important requirements of the Act in relation to confidentiality are:

- ❖ Data kept on an individual should be done with the **consent** of the individual. (You may have noticed that you are often asked to agree for information about you to be stored and for it to be used by other organisations.)
- ❖ Data on individuals should **not be given to others** without the consent of the individual.
- ❖ Data should only be collected on individuals that is **needed at that time**.
- ❖ Data on individuals must be **checked with the individual for accuracy** and must be **kept up to date**.
- ❖ Data on individuals should only be **kept for as long as required** (e.g. personnel records are kept for seven years after the person has left the organisation).
- ❖ Data should be **secure**.
- ❖ Sensitive data such as racial or ethnic origin, membership of trade unions, physical or mental health conditions and information on criminal offences are subject to special treatment.

(Continued on page 5)

- ❖ Personal data can't normally be transferred outside the European Economic Area (the 25 European Union Members plus Iceland, Liechtenstein, and Norway)

The **Human Rights Act 2000** is based on the European Convention on Human Rights, which the UK helped to write many years ago. It has now been made part of UK law, giving people greater opportunity to use it to claim specific rights, including certain rights to privacy, which employers need to respect. The Human Rights Act is being used to help define more clearly people's rights to privacy, but this is still developing.

How is confidentiality enforced?

Confidentiality is enforced through the three main types of regulation that you have already found out about. If confidentiality is not maintained the individual has the right to complain and, in serious cases, to take legal action.

Exercise

1. Pat and Leslie have used the work Email system to talk about a discipline case that Pat is giving evidence at.
2. Jo has asked the personnel department for Miriam's address so that she can send Miriam a get-well card.
3. In a pub you overhear a social worker talking to her friend about a child she is involved with at work, mentioning the child's name and giving lots of confidential details.

As the leader of the team these people work in, decide in each of the examples, which regulation(s) the team members have probably breached and how you would deal with it.

Case	Regulation(s) breached?	How you would deal with the breach?
1		
2		
3		

You may well have suggested the following points in relation to each of the examples:

1. Using email to talk about a confidential matter is almost certainly a breach of organisational policy. The organisation's discipline procedure will state that matters to do with discipline cases are confidential. You should tell Pat that she should not be discussing this with Leslie.
2. Miriam will have given her address to personnel as part of her confidential record. Although Miriam may not have minded her address being given to Jo, under the Data Protection Act the department cannot give her address to clients or members of staff. Suggest to Jo that she asks Personnel to send the card to Miriam for her (and stamps it herself).
3. There are two issues here. Firstly the social worker is in breach of her professional code of practice that states that matters relating to clients are confidential and can only be discussed with parties involved and other appropriate professionals. Secondly, the social worker could well have breached the Data Protection Act and possibly the Human Rights Act. This is potentially a very serious matter and could lead to suspension and legal investigation. You should refer this to a manager.

Information, security and the Internet

Many organisations these days have information on their **Internet website** which they want people to see. The Internet is a way of linking computers all over the world through telephone lines and other, high speed, connections.

If your organisation sends and receives information using the Internet it may have in place a **secure site** so that unauthorised people cannot have access to the information collected on it.

A secure site is a site which allows people to provide their personal details to an organisation with the guarantee that no one else using the Internet will be able to get to the information. This would be useful if your organisation sells goods over the Internet by credit card, or invites people to give their name and address so that information or goods can be sent to them by post.

In sites that are not secure it is possible for someone with the expertise to gain access to an organisation's database and obtain all the information it holds about its clients. Identity theft and the misuse of credit cards are rapidly increasing as more and more information

Handling confidential information



about us is collected, stored and transferred electronically, making confidentiality and security major issues for all organisations.

But it's not only outsiders who are a threat to confidentiality - employees can be as well. Because of all the important information which can be stored on computers, a **confidentiality policy** is a way of making clear to employees their responsibility for not disclosing this information to unauthorised people, or looking at information they are themselves not authorised to see. If employees don't keep to the organisation's confidentiality policy it can result in instant dismissal or even prison. The costs to a company can also be enormous (in monetary terms and reputation) if information which should be confidential is disclosed improperly.

Case Study

One Friday afternoon, Jane overheard the Personnel Manager say that the organisation had a cashflow problem and that if sales did not pick up over the next few months the organisation would be in serious trouble. It could even be forced to close with millions of pounds of outstanding debts. Jane couldn't believe what she had just heard and was bursting to tell her colleagues.

She went back to her computer and sent an e-mail to one of her colleagues explaining what she had just heard. Her friend then forwarded the e-mail message on to someone else.

By the end of the day the rumour was known by everyone in the factory and some people outside.

Monday morning came and many of the shareholders in the company began to sell their shares, the company was now facing disaster. The management had traced the disclosure of the information to the e-mail that Jane had sent. She was called into the Manager's office and dismissed instantly. However, it was too late to repair the damage done to the organisation and it was forced to close.

Whistle-blowing

The **Public Interest Disclosure Act** (Public Interest Disclosure Order in Northern Ireland) came into force in 1999. This protects people at work who have genuine concerns about **malpractices** at work. Malpractice includes things such as crimes, civil offences (like breaches of contract), miscarriages of justice, danger to health and safety or the environment or the covering up of any of these. The law encourages people to raise concerns about malpractice in the workplace.

Handling confidential information



If you think that there are malpractices in your workplace, you should first of all tell a relevant manager. If no action is taken you can seek legal advice. It doesn't matter if the information is confidential. If you suspect malpractice, you have a right to seek advice. The best place to go is Public Concern at Work (www.pcaw.co.uk), which is a legal advice centre that specialises in whistle-blowing. You are protected in law from any reprisals by your employer if you approach them or another legal adviser, including seeking the advice of a trade union.

If you find that your employer takes no action despite your warnings, you are also protected if you go public (blow the whistle) on the malpractice. The law protects whistleblowers from dismissal and victimisation because it is believed to be in the public interest for malpractice to be dealt with.

Freedom of information

The **Freedom of Information Act 2000** gives any person the legal right to ask for and be given information which is held by a public authority. If you work for a public authority, such as the civil service, a local council, a school or hospital, you may have already learnt that all information held by the organisation could be asked for by the public. There are exemptions for:

1. information which might harm the public interest, such as national security or international relations;
2. information which may not legally be disclosed;
3. personal information about other individuals;
4. information which is confidential, such as commercial contracts.

If you work in a public sector organisation you should be aware that any document you produce or handle may be disclosed. It is only confidential if it meets one of these four criteria.

How do you handle confidential information?

This session has helped you to identify the differences between confidential and non-confidential information at work. You should be clearer now about your role in maintaining and ensuring confidentiality. In particular, by making sure that you keep to the law that regulates the use of information at work.

Comprehension Check

Complete the following exercises. Refer back to the session if necessary.

A. Information is likely to be confidential if it is about:

1. _____
2. _____
3. _____

B. What are the four main laws affecting confidentiality?

1. _____
2. _____
3. _____
4. _____

C. Complete each sentence. Circle the letter in front of the answer.

1. The Data Protection Act:
 - a. only covers computer records.
 - b. only covers non-computer records.
 - c. covers computer and non-computer records.

2. The Data Protection Act:
 - a. has been replaced by the Human Rights Act in 2000.
 - b. was updated in 1998.
 - c. doesn't apply inside the European Union.

E. Mark the following statements (T)True or (F)False:

1. Data kept on an individual doesn't need their consent.
2. Data on individuals can be given to others without their consent.
3. Data should only be collected on individuals that is needed at that time.
4. Data on individuals must be kept up to date.
5. Data on individuals should only be kept for one year.
6. Data should be secure.

Making Connections

Answer the questions following the case.

Hasim has only just started working in Helen's team in the factory. He is very keen but he gossips all the time. Helen is getting increasingly irritated by it, but nobody else in the team seems to mind. In fact, they are all keen to hear what he has found out today. Jan, another team member, says that he's better than her magazine, because all his gossip is about people she knows in town or in the factory.

Hasim's job is to collect parts for the team and to take finished work to other parts of the factory. He also records the details of what the team has produced on the computer terminal. One reason why he finds out so much is that he is always moving around the factory. Helen can't fault him for his work because he manages to work and talk at the same time.

Helen decides to turn a blind eye to his gossiping, until she overhears one of her team talking about a friend of Helen's. She says that this friend has asked for some compassionate leave because her husband is dying of cancer. Helen knew this. She also knew that her friend wanted it kept secret, as her children hadn't realised how serious it was.

Helen asks her team member where she heard this. She says: "From Hasim of course. Where else?" and laughs.

Helen decides to approach him about it. Hasim says that he was told by his girlfriend. Helen knows that she works in the Personnel Department.

- ❖ What should Helen do now?

- ❖ Is there anything that Helen should have done earlier?

Think and Apply

How well do you use the skills in this session? Think about the information that you handle.

- ❖ Do you always think about its confidentiality?
- ❖ Is there anything which you or your team do which might need to be changed to ensure that confidential information is better protected?

1. Read the list of skills. Tick the boxes to show your strengths and weaknesses.

Skills	strengths <- - - -> weaknesses			
	I'm good at this	I'm quite good at this	I'm not so good at this	I'm quite poor at this
■ recognising what information is confidential	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
■ knowing the different types of regulation about confidential information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
■ appreciating how the law governs confidential information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Do you want to improve any of these skills?

3. How do you plan to improve the skills you listed in question 2? (You might want to discuss this with your line manager or your tutor/mentor/coach.)