7. CONFIDENTIAL INFORMATION

7.1 Introduction

7.2 Confidential Disclosure

7.2.1 Controlling disclosure of confidential information
7.2.2 Implied confidence
7.2.3 Releases from confidentiality
7.2.4 Springboard principle

7.3 Employees

7.3.1 Current employees
7.3.2 Ex-employees
7.3.3 Implied obligations of ex-employees
7.3.4 Employees and notice period

7.4 Confidential Computer Programs

7.5 Unwanted Confidences

7.6 Managing Confidential Information

7.7 Know-how and show-how

7.8 Legal Remedies

7.9 Confidentiality in other countries

7.10 Summary of confidentiality

CONFIDENTIAL INFORMATION

7.1 INTRODUCTION

What is confidential information?

- Collection of data's or any information that should be kept confident are termed as confidential information.
- There are no specific law followed for this like other IPR.

What kind of information can be kept confident?

Information related to the trade secrets, processes, operations, style of works, or apparatus, or to the production, sales, shipments, purchases, transfers, identification of customers, inventories, or amount or source of any income, profits, losses or expenditures of any person, firm, partnership, corporation, or other organization, or other information of commercial value

What cannot be kept confident?

Once information is available to the public it cannot be 'made' confidential again.If process details are described in a published paper, one cannot then oblige others to keep them secret. Anything that is made known to the public cannot be kept confident again.

Eg: Inventions made centuries before.

7.2 CONFIDENTIAL DISCLOSURE

7.2.1 Controlling disclosure of confidential information
7.2.2 Implied confidence
7.2.3 Releases from confidentiality
7.2.4 Springboard principle

7.2.1 Controlling disclosure of confidential information

- The best method of keeping a secret is not to tell anyone, but in an engineering environment it is often essential to disclose sensitive information to other companies or to individual consultants.

- A supplier may need to be told in detail of the proposed use of a component or a potential purchaser may ask for the test results on a new device. In both cases, confidential information will be handed from one company to the other.

- The disclosing company's position can be protected by a confidentiality agreement, a written record setting out briefly what the information is, who it is being supplied to and the reasons for the supply.

- The company receiving the information signs the agreement, and should keep a copy as a record.

- Transfer of confidential information may also occur by observation.

Example
A visitor being shown round company premises may observe work in hand, such as a relevant manufacturing technique or even the name of another customer or supplier.A visitor's confidentiality agreement can be used, which the visitor signs as a promise to keep confidential all the information received while on the company's premises.

- The flow of confidential information can be two-way.

Example

Two companies may be considering a joint venture (JV) of some sort and will need to disclose their current levels of expertise to each other. Each can then promise to keep received information confidential and to limit its use to evaluation of the potential JV. If it goes ahead, a much more detailed legal agreement will be needed.

Format of agreement

- The length and level of detail of a confidentiality agreement is very variable.
- There are few standard terms relating to such agreements.
- Usually the wording is negotiated by those involved or their legal representatives.
- The length of time the agreement lasts should be the period during which the information will be important, plus a safety factor.

7.2.2 Implied confidence

- It includes unplanned disclosure of information.
- In an enthusiastic discussion between engineers, more may be said than is commercially wise. Sometimes a problem is solved on the spot and a possibly patentable invention is made and disclosed verbally.

Example

Saltman Engineering Company Limited prepared drawings of tools for the manufacture of leather punches and placed a contract on Campbell Engineering Company Limited to make the tools. Campbell produced 5000 punches under the contract, but also made and sold 8700 additional punches. The Court of Appeal decided that, although the contract was silent on confidentiality, it

was an implied term that the drawings were confidential documents. This was so even though the punches themselves could now be regarded as public knowledge. Campbell had breached an obligation of confidentiality owed to Saltman.

- It is highly advisable to record the position in writing and a signature should be obtained to confirm that the other party agrees to the implied position.

Tender

- In situations such as competitive tenders, where confidential drawings and specifications are sent to several companies, strong conditions of confidence should be imposed.
- These should make it clear that the information is provided only so that a tender can be made and so that the winner can fulfil the contract.
- All potential tenderers should also agree to return all documents on failing to win the contract.

7.2.3 Releases from confidentiality

- If confidential information is published in some way it can never be retrieved and made secret again.
- This is a weakness of this type of legal protection and, therefore, particularly careful management practice is needed the recipient of the information is the cause of it becoming public, the obligation should still bind that company.
- Typical release clauses are given below:

RELEASES FROM CONFIDENTIALITY
The obligations imposed by this Agreement shall not apply to:

(a) information which is already in or becomes part of the public domain without fault of the Recipient;
(b) information which can be shown by documentary proof satisfactory to the Discloser to have been in the possession of the Recipient before disclosure by the Discloser;
(c) information which can be shown by documentary proof satisfactory to the Discloser to have been generated independently by the Recipient;
(d) information which has come into the possession of the Recipient from any third party without breach of any confidential relationship

RELEASE CLAUSES

7.2.4 Springboard principle

- Information received in confidence must not be used in an unfair way after it has become publicly available to some extent.

Example

The buildings were developed by Terrapin Limited and full details were given to Builders Supply Company (Hayes) Limited as part of a manufacturing contract. Some of the buildings were made by Builders Supply for Terrapin, but Builders Supply then began to make the buildings for sale on their own behalf. Terrapin objected, arguing that their confidential information was being misused. Builders Supply pointed out that the details of construction were disclosed in the buildings as sold, so the information was no longer confidential. The decision of the court was that Builders Supply had misused the confidential information.

7.3 EMPLOYEES

7.3.1 Current employees
7.3.2 Ex-employees
7.3.3 Implied obligations of ex-employees
7.3.4 Employees and notice period

7.3.1 Current employees

- Employed engineers have an obligation to protect their employer's confidential information. This is known as a 'duty of fidelity' or 'faithful service'.

- An employed engineer must not disclose confidential information which he or she acquires as a result of that employment, whether the information is received from the employer, from a third party as part of the employment duties, or is generated by the engineer during professional activities.

- Nor should an employee use confidential information for his or her own personal benefit, even if such use does not involve disclosure to others

Example:

In a case in 1946, Mr and Mrs Davis worked for a company called Hivac, which made valves for hearing aids. They wanted to work for a competitor company, Park Royal Scientific Instruments, in their spare time. The court restrained them from doing this. There was no evidence that they would disclose Hivac's confidential information to Park Royal, but there was a serious possibility of conflict of loyalty.

The duty of an employee covers the disclosure of information to an employer as well as maintaining confidentiality.

Example:

In a case relating to a type of above-ground swimming pool, Mr Bryant was managing director of Cranleigh Precision Engineering Limited, the manufacturer of the pools. He found out about a patent owned by a Swiss company which was potentially damaging to Cranleigh. He did not tell his employer, but left the company and tried to acquire rights

under the patent to set-up in competition. The court found he had no right to do so as he should have told Cranleigh that the patent existed.

7.3.2 Ex-employees

- Engineers frequently change employment.

- The ex-employer may be concerned that company secrets depart with the person. When an engineer changes employer, he or she may continue to use engineering expertise, the sort of thing which has been referred to as 'ordinary skill and knowledge' or an engineer's 'stock in trade' or 'skill and dexterity, manual or mental ability'.

- What an ex-employee cannot do is use the trade secrets of the previous employer, or other equally important information, to give an unfair competitive advantage to the new employer.

Example:
A salesman will know customer names and addresses merely from frequent contact with them and would be restrained from disclosing them while employed, but would be far less restricted after employment ceases on the pragmatic basis that memory cannot be deleted. But supplementing memory by written records is not allowed.

In a case where documents were copied and taken away, the court held that this was wrong and that using the copied information to supplement memory was unfair – it acts as a springboard for the new employer. Taking copied papers is of course both infringement of copyright and theft, which may have influenced the decision. The judge said-

"If an employee is sufficiently ill-advised to remove his employer's property when he leaves and that property contains information which

was confidential during the course of his employment, he may by reason of his own wrong thereafter be restrained from doing something which, but for his own wrong, he might have been entitled to do."

7.3.3 Implied obligations of ex-employees

Three clear but limited principles apply to ex-employees:
• An ex-employee must not use or disclose trade secrets of a previous employer.
• An ex-employee must not carry away copies of records for future use.
• An ex-employee can be subject to reasonable restrictive covenants.

Example:

The dispute arose between the company Faccenda Chicken Limited and one of its ex-employees, Mr Fowler. Faccenda's business was breeding and slaughtering chickens, and selling them chilled but not frozen. Mr Fowler had been the sales manager and had the idea of using refrigerated vans for direct supply to supermarkets and butchers. Over several years he built up a profitable operation for Faccenda based on ten vans, each driven by a salesman round a particular area of the Midlands. The salesmen-drivers quickly learned the customer names and addresses, the quantities and qualities required by
them, the days and times of day each customer required a delivery, the prices charged to each, and the best routes to follow. Mr Fowler and Faccenda then parted company. Mr Fowler set-up a rival operation,
in the same areas of the Midlands, using refrigerated vans to supply many of the same customers, often at lower prices. He advertised for staff, and eight people, five of them salesmen-drivers, left Faccenda and joined him. Faccenda sued Mr Fowler, arguing breach of confidence by misuse of the sales information about routes, particularly the information about prices charged. Faccenda lost in the High Court, appealed, and lost again.

Factors include:

1. The nature of the employment: if confidential material is handled frequently, there will be a greater obligation of confidence after employment ends. The employee will realise the sensitive nature of the material, in contrast to an employee who rarely handles confidential material. In the Faccenda case, none of the van drivers
2. The nature of the information: some information, while not classifiable as a trade secret, is so highly confidential that it requires the same protection as a trade secret. If information falls into that category, an ex-employee can be prevented from disclosing it. In the Faccenda case, the pricing information was held to be of such a nature that it could have had the same protection as a trade secret if it had been properly handled by the company. But Faccenda did not take any steps to protect the information.
3. Whether the employer impressed on the employee that the information was confidential.
4. Whether the information was separable from other information.

As mentioned above, handling information in a way which indicates its value will help to place greater obligations on an ex-employee. Faccenda did not issue warnings and did not keep the pricing information separate. The case still does not provide a definition of 'trade secret' but it gives some useful practical guidance on handling secrets. The principles have been approved and reapplied in many subsequent cases.

7.3.4 Employees and notice period

When an employed engineer gives notice of an intention to leave a company, there is still a duty of good faith to the employer, but it may be less than if notice has not been given. If an engineer starts to set up a competing business in the notice period, under a court decision this is quite permissible. What is not allowed are attempts to entice customers to a new company or making copies of useful records to take away.

7.4 CONFIDENTIAL COMPUTER PROGRAMS

- If software is specially written for a company, only the software developer will have the knowledge or expertise to cure a fault. This is because only the developer is familiar with the source code from which the object code is derived.
- Software developers protect their expertise by keeping their source code closely confidential.
- If the program is important to the user company, and especially if the developer is a small firm whose financial future is not secure, the user may want to ensure that the program can still be maintained even if the small firm vanishes.
- The usual compromise between confidentiality and security of the user is to set up an escrow arrangement. A copy of the source code is placed with a trustworthy third party who keeps it confidential until a certain event occurs, such as the developer becoming insolvent, when the copy is released to the user who may then study it and maintain the program when a fault arises.
- Advice on escrow schemes can be obtained from the National Computing Centre website at www.ncc.co.uk under Services. Sometimes a bank or a solicitor is asked to hold the escrow copy – this is acceptable provided conditions which are physically suitable for storage of software can be ensured.

7.5 UNWANTED CONFIDENCES

Many engineering companies, especially large ones with a high public profile, are offered ‘good ideas’ by members of the public wishing to be helpful. Most of these suggestions are technically impractical or impossible, but occasionally a suggestion is genuinely useful. Frequently, the ideas are offered only on condition that they are received in confidence.

The risk for a company is that the genuinely useful idea is already being developed in-house, but that the person making the suggestion does not believe this and accuses the Company of breach of confidence. Alternatively, the proposal is sometimes merely a 'wish list', long recognized by the industry as being desirable, but barred by a technical problem. If the company later comes up with a practical solution, again the individual making the suggestion may accuse the company of stealing the idea.

One solution is to accept an idea from outsiders only if there is no obligation of confidence. This is likely to discourage most offers. An alternative is to agree to look at suggestions only if a patent application has been filed first; the application acts as a record of the idea and bears an official date-stamp. But the individual must invest either time in preparing his or her own patent specification, or must pay substantial professional fees. Contribution of ideas is again discouraged.

Neither of these approaches provides an answer if the letter offering the idea contains a description of it. If a company employee reads the letter, the information has been transferred into the company and the ground laid for arguments of breach of confidence.

One way round this is to have all letters which look as if they might be offering ideas to be opened by non-technical staff. The company can then argue that whoever read the letter did not understand the technical content, so the company has not received the information.

The policy for dealing with such unsolicited technical suggestions depends on whether the company wants to discourage them by strongly worded refusals to accept the information in confidence, or to encourage them by politely pointing out the position and suggesting that the writer re-submits the idea in a way acceptable to the company.

7.6 MANAGING CONFIDENTIAL INFORMATION

The ultimate test to apply to information is 'would a judge agree that this information deserves legal protection by confidentiality?'. The judge will not be convinced of this if the company claiming to own it did not

treat it as secret until too late. A thread running through many legal decisions is that the information must be managed appropriately within a company if it is to benefit from the protection of the law of confidence. A list of practical steps which can be taken is given below.

Marking. Papers and computer records which are regarded as important can be marked, for example, 'commercial in confidence'. If necessary, access can be restricted, for example, to named people. Copies can be numbered and recipients noted. A company should devise a policy on handling such documents – possibly they should be locked away each night, or not left on a desk in an unoccupied office. Obviously, not all papers need to be treated in this way. The inconvenience would be unjustifiable, and the message of treating some information with special care would be diluted or lost.

Separating important information. If information is of great importance it should be kept separate from other information. Documents which are generally available should not include confidential items.

Reminders to employees. Although employees have an obligation to their employers to keep company information confidential, it is prudent to remind them of this. Different levels of staff within a company will need to be reminded at different frequencies. A chief engineer will be handling company secrets on a regular basis, while young support staff will be less aware of their obligations, so a reminder to them associated with a particularly sensitive project may be beneficial.

7.7 KNOW – HOW AND SHOW – HOW

Know-how, the application of technology to a practical situation, can often be valuable but it certainly need not be novel, and may only be protectable by confidentiality. It is defined in an EU regulation as 'secret, substantial and identified in any appropriate form' which has the

implication that there must be a record. Some types of information can only be demonstrated, and the word 'show-how' is sometimes used for them.

Even though know-how and show-how are difficult to define, both can be confidential. They are often transferred from one company to another, for example, as part of a licence agreement, by visits of engineers to the recipient of the information to give technical training and demonstrations. Such visits can also be covered by confidentiality agreements.

7.8 LEGAL REMEDIES

If an engineering company's confidential information is disclosed in some way, either by publication, demonstration or transfer to another company by an ex-employee, it is rarely possible to make the information confidential again, but some legal action can be taken. If the parties cannot negotiate a settlement, formal legal proceedings can be started.

There are three requirements:

- The information must have been confidential.
- The information must have been disclosed in circumstances which impose an obligation on the receiving party to keep it confidential.
- The obligation must have been breached.

These include payment of damages and an injunction to stop further disclosure or further misuse.

A disadvantage of confidentiality as a form of protection is that third parties who receive the information innocently, without any notice or implication that it is confidential, cannot be stopped from making further use of it. However, the party which has caused the breach of confidence can be restrained from further use and is thus put at a disadvantage.

7.9 CONFIDENTIALITY IN OTHER COUNTRIES

General

- In other parts of the world the existence of a law of confidentiality, and even local comprehension of the concept, varies widely.
- In continental Europe, the law is civil law.
- In the USA, the applicable law is state law, not federal law
- Unlike other IPRs there are no direct international conventions relating to confidential information

TRIPS

- Under the TRIPS Agreement, undisclosed information – trade secrets and knowhow – must be legally protectable, on condition that it is secret that it has commercial value by reason of the secrecy, and that reasonable steps have been taken to keep it secret.
- A person lawfully in control of such information must have the possibility of preventing it from being disclosed to or used by others without consent, in a manner contrary to honest commercial practice; this will cover breach of contract and breach of confidence.
- Local advice in every country is particularly important for this area of law.

7.10 SUMMARY OF CONFIDENTIALITY

Any type of information which is not available, or not easily available, from another source can be protected by confidentiality. If valuable information is to be disclosed to a third party the best practice is for the recipient to sign a confidentiality agreement in advance, agreeing not to disclose or misuse it.

Employees have an implied obligation to protect confidential information belonging to their employer, but the obligation is lower when the employee leaves the company. The way information is handled

in a company can affect the implied obligation on employees to treat it as confidential.