Filing and records management

Filing and records management is a vital — if uninspiring — part of any business. Information is a major element in many companies' competitive advantage, but it can only be utilised if it is available when needed.

At the same time, every business can benefit from cutting the wasted effort associated with looking for misfiled information and misplaced files. The same principles apply to both computer and paper records.

This briefing outlines:

- How to organise your business records.
- How to maintain security — and comply with the Data Protection Act.
- Archiving for long-term storage.
- How long specific records must be kept.

1 'Family-tree' filing

You will need one single filing and records system to ensure that people can find the information they need, when they need it.

This system is usually based on a hierarchy, or family tree, of files.

1.1 Decide the **main categories** for your filing system. Give each a code.

- For example, sales (SA), accounting (AC), human resources (HR) and general administration (GA).
- Have a Project Files category (PF) for whatever falls outside your main categories.

1.2 Divide each category into **sub-categories**.

- For example, divide HR into HR/recruitment, HR/pay, HR/performance appraisals, HR/training, HR/employee file.

1.3 Further divide these sub-categories into **sub-sub-categories**, to whatever level is necessary.

- For example, if you need to file the CV of a potential secretary (for the first time), you might create a new file called HR/recruitment/candidates/secretary/potential.

1.4 **Store files** where they are needed, in alphabetical order.

For example, if customers have named files, these can be stored near the sales team, in order eg SA/customer/Amis.

1.5 Businesses with large or complex filing systems often use a **filing code** instead of a name.

- For example, potential secretary candidates might be filed in HR/1/2/1/1 (where the first 1 signifies recruitment, the 2 means candidates, the next 1 means secretary and the last 1 means potential).

2 Managing the system

2.1 Give one person overall **responsibility** for your filing and records system.

- Make each manager and individual responsible for managing information within the context of his or her job.
- All records should be available to all staff who need them to carry out their work (with appropriate and necessary safeguards for personal and sensitive information).
- Communicate the basics to all employees.

Filing dilemmas

A Some information needs to be **split** between two files.

For example, notes about the IT training course that your employee, Smith, has just completed.

- Record the usefulness of the training course in the HR file HR/training/IT. But record how Smith performed on the course in Smith's personnel record — HR/employee file/Smith.

B Some information needs to be **copied** into two files.

For example, as well as filing it in the accounts department, you might need to copy an invoice (or an order) to your sales and distribution departments.

C Problems occur when people do not file items within the main **system**.

- For example, when the person running a training project effectively sets up a second filing system, filing all the information in his or her own 'work-in-progress' file. Or if the information is all filed under Project/training, thus ensuring that this information is never united with related information in the main Training files. The danger is that almost anything at all can be put under the Project category.

2.2 Ensure that **new files** are only created with specific approval of the person responsible.

2.3 Good **indexing** and **titling** are essential.

- A file's title must be meaningful and must accurately reflect its contents.
- Anyone who knows your system ought to be able to go straight to the right file nine times out of ten.
- If the nature of the contents shifts, the file's title should not usually be changed. It is better to open a new file.

2.4 Develop a clear **tracking system** for files.

- Ensure that files which are removed from their normal locations are signed out, so that they can be traced.

2.5 Do not allow files that spring up around **projects** to undermine the system.

- Make moving project data into the main filing system the final phase of any project.

2.6 Discourage the growth of **personal filing** systems (see box).

3 Making it work

3.1 Write **file names** on the spines of (narrow) folders or ring binders, writing from the top downwards. Consistency means all the titles on a shelf can be read at once, at a glance.

3.2 If it is not obvious, put an outline of the **contents** on a record sheet in the front of each file, with dates for each update.

3.3 Use **colour** to make files easier to use.

- Use a differently coloured file for each category. For example, red for sales and green for accounting.
- Use coloured dividers to separate sections.
- Use coloured paper (or mark the top right corner with a highlighter pen) for important documents. For example, an invoice, a contract, or a progress summary.

3.4 Do not let working files get **too fat**.

- Papers in a file will start to be damaged once it is more than about 3cm thick. Close the folder (insert a sheet saying 'Folder closed, see Part 2'), mark it 'Part 1' and open a new folder for the same file (marked 'Part 2').

➨Advice and guidance is available from the Society of Archivists www.archives.org.uk and the Records Management Society www.rms-gb.org.uk

3.5 Where documents are **created electronically**, store them on PC hard drives or on local servers where employees can access them — subject to appropriate accessibility rules.

- Discourage employees from saving work-in-progress and other files to their PC desktops. Files saved to the desktop may not get backed-up and could be permanently lost should the PC fail

3.6 Records of **one-off enquiries** that do not fit in anywhere else should be filed in date order in a 'general enquiries' folder.

- These records should be destroyed after a short time (eg six months), if the enquiry has not come to anything.
- One-off sales enquiries are different. They should be archived for the previous five years. You may be able to sell your new products to these old enquirers.

Six filing guidelines

A Know **what** you have got.

- Even in the smallest businesses, people often waste hours collecting information the business already holds.

B Know **where** information has been put.

- If you cannot find your research data on customer order sizes, you cannot use it to plan your marketing.

C **Store** information efficiently.

- Make sure the system you use closely matches the needs of your business. For example, an employment agency will need vast 'people' and 'pay records' categories, with room for many sub-categories beneath the main headings.
- Files on computer take up a tiny physical space and can be shared easily and searched quickly. It may be worth scanning paper files for computer storage, or microfilming them, if you hold large amounts of paperwork. For example, in an insurance brokerage.

D **Use and re-use** the information that you have captured.

- Data filed on a computer database can be 'sliced' in different ways and viewed from several angles to yield different types of information for different business purposes.

E Do not **hold on** to records longer than you need to (see **6** and **7**).

F **Dispose** of old records safely (see **4.5**).

- Personal files and commercially sensitive material must be shredded.
- Consider recycling, where appropriate.

➨Training for business administration NVQs is widely available and can cover all aspects of filing and records management.

4 Security

In any business, some information needs to be kept confidential, with access restricted to certain employees, or kept from outsiders.

Files which may be taken home, whether by directors, managers or junior employees, are a particular security risk.

4.1 Confidential **documents** must be kept in locked cupboards or filing cabinets.

- Have a simple way of classifying and marking confidential files. For example, by adding an asterisk after the file's name.

4.2 Confidential material in **computer files** can be given appropriate levels of protection.

- Protect files with a password.
- Files can be compressed and password protected, using utilities such as WinZip.
- If appropriate, encode high security files, using encryption software.
  Even free encryption software can give almost unbreakable protection.
  Free software can be downloaded from reputable sites such as www.tucows.com or www.download.com.

4.3 You must have **back-up** systems in case of loss, theft or damage to files.

- Regular computer back-ups are essential.
- Back-up copies of important files must be stored in a secure, off-site location.

4.4 Install virus **protection** to safeguard information stored on computer.

- You may want to consider installing a security 'firewall'.

4.5 **Dispose** of old files and computers containing confidential information in a secure fashion.

- Paper records should be shredded or disposed of through a recognised waste contractor.

- Hard drives on redundant PCs should be reformatted to make all the data on them unretrievable. Otherwise all emails, for example, will effectively be retained forever.

5 Legal issues

5.1 The **Data Protection Act** covers how you must handle and store personal information.

5.2 You are legally required to keep specified **tax and financial** information for a set period (see **7**).

5.3 If you hold **confidential** information which could damage others, you may have a legal duty to take extra security measures.

5.4 Include clauses restricting how **employees** may use company information in each person's terms of employment.

- For example, sales people may try to take a copy of the sales database when they leave.

6 In the longer term

6.1 Be clear about **how long** you want to keep different types of file — for your own business reasons — and how long you are compelled by law to keep them (see **7**).

- Keep long-term records in good condition by storing them in boxes.
- Move old records out of the main filing system and into an archive to cut costs and storage requirements. This helps keep the filing system efficient and uncluttered.

6.2 Apply sensible **disposal schedules** that encourage people to get rid of material as soon as it is clearly not going to be needed.

6.3 For long-term storage, consider **scanning** paper files into computer files.

6.4 If you need access to a lot of archive files, consider using a **records management** company.

- Each file is bar-coded and stored ready for immediate delivery to you when required.
- The legal, accounting and insurance companies use these services, as they cannot afford to mislay customer records. Record management companies offer consultancy services and can work with other suppliers (eg software houses) to provide an integrated service.

7 How long is long-term?

7.1 **Accounting** records for an ordinary limited company must be retained for three years.

- There is no legal minimum period for sole traders or partnerships.
- Plcs must keep accounting records for six years.

7.2 Sickness and **sick pay** records, and records relating to **maternity pay**, **paternity pay** and **adoption pay**, must be retained for three years.

7.3 **Pay** records must be kept for a minimum of three years after the end of the tax year the earnings relate to.

7.4 **VAT** records and documents must be kept for six years.

7.5 **Contracts** must usually be kept for six years, though contracts under seal must be kept for 12 years.

7.6 **Tax** records must be kept for at least six years, as HM Revenue & Customs can raise assessments up to six years after the end of the period the assessment relates to.

- There is no legal time limit (in effect, it is 20 years) in cases of tax fraud.

7.7 Where there have been any problems, such as industrial injuries, **health and safety** records should be kept for at least 12 years, as claims for personal liability can be lodged up to 12 years after the event.

- Records relating to some hazardous substances, for example, asbestos, may need to be kept for up to 40 years.

7.8 The requirement to retain your compulsory **employers' liability insurance certificates** for 40 years ended on 1 October 2008.

- Employers are still required to display their certificate of insurance at each place of business.
  The certificate can be made available to employees electronically providing all employees can gain access to it.

This publication is for general guidance only. The publisher, expert contributors and distributor disclaim all liability for any errors or omissions. Consult your local business support organisation or your professional adviser for help and advice.