Think Ahead **ACCA**

Guide from

Clear House Accountants Tel: [+44(0)2071172639] Email: [info@chacc.co.uk]
[https://chacc.co.uk]
[Business Advisors and Accountants in London]

Filing and records management

Business information can be an important contributor to your competitive advantage. Good filing and record-keeping systems make sure you have what you need, and avoid wasting time and effort looking for misfiled information and misplaced files.

A simple approach can help you organise both computer and paper records. You also need to make sure your information is secure and that you are complying with your legal obligations.

1. 'Family-tree' filing

You 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.

Decide the main categories for your filing system and 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.

Divide each category into sub-categories

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

Further divide these 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.

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.

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

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).
- Make sure that all managers and staff handling personal data are aware of your obligations and the rights of individuals under the EU General Data Protection Regulation (GDPR) and of any specific data protection policies and procedures you may have.
- Consider appointing a Data Protection Officer (DPO) to oversee all aspects of your data protection compliance, including your filing systems.
- Communicate the basics to all employees.

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

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.

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.

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

- If any new project involves personal data, take a 'privacy by design' approach, conducting data protection impact assessments where appropriate, to ensure that personal data is protected.
- Make moving project data into the main filing system the final phase of any project.

Discourage the growth of personal filing systems

- See Filing dilemmas.

Filing dilemmas

Some information needs to be split between two files

For example, for 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.

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.

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.

3. Making it work

Write file names on the spines of (narrow) folders or ring binders

- Write from the top downwards. Consistency means all the titles on a shelf can be read at once, at a glance.

If it is not obvious, put an outline of the contents on a record sheet in the front of each file

- Include dates for each update.

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.

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').

Store electronic documents where employees can access them

- Files can be stored on a network server so that everyone can access them, subject to appropriate access controls.
- 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.

Use a 'general enquiries' folder for one-off enquiries that do not fit anywhere else

- File the records in date order.
- 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.

4. Security

In any business, some information needs to be kept confidential and personal data needs to be protected, 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.

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.

Confidential material in computer files can be given appropriate protection

- Protect files with a strong password. Use a combination of letters, numbers and special characters. Avoid anything that can be easily guessed or 'cracked'. Use a [tool](#) for testing your password security.
- Files can be compressed and password protected, using third-party utilities such as WinZip, or using features built-in to Windows and macOS.
- If appropriate, encode high security files, using encryption software. Even free encryption software can give almost unbreakable protection.

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

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

Limit the storage of data on laptops and other mobile devices

- Discourage (and prohibit, where appropriate) employees from storing personal and/or confidential data on laptops and other mobile devices that can be easily lost or stolen.
- If storing personal data on a laptop or mobile device, ensure that the device's storage (eg HDD or SSD) is encrypted and that the device itself is protected with a strong password or biometric security such as a fingerprint.
- Be wary of over-hyped new security measures that can, in reality, be easily compromised such as facial recognition technology that can be bypassed with a photograph.

Install virus protection to safeguard information stored on computer

- Computers connected to the internet should also be protected from unauthorised access with a security 'firewall'.

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 physically destroyed or securely 'wiped' to make all the data on them irretrievable. Otherwise all emails, for example, will effectively be retained forever.

5. Legal issues

The GDPR covers how you must handle and store personal information

- Amongst other things, you must only keep personal information you need, ensure that it is held securely, and delete or otherwise dispose of it when it is no longer necessary. The retention of personal data should be regularly reviewed to ensure that it is not being held for longer than necessary.
- Where any personal information is to be used for a project, make privacy and data security key aspects of the planning process from an early stage.
- Individuals have a range of rights under the GDPR including (but not limited to) the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to object to processing, and the right to data portability. All of these rights may have an impact on your filing and records management as you will need to respond quickly when an individual chooses to exercise one or more of their rights.

You are legally required to keep specified tax and financial information for a set period

- See How long is long-term?

In any business, some information needs to be kept confidential

- Access may need to be restricted to certain employees or kept from outsiders.

Include clauses restricting use of company information in 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

Be clear about how long you want to keep different types of file

- Take into account both your business needs and how long you are compelled by law to keep them.
- Keep long-term records in good condition by storing them in boxes. Consider scanning paper files into computer files.
- 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.

Apply sensible disposal schedules

- Encourage people to get rid of material as soon as it is clearly not going to be needed.

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.
- 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.
- If personal data is involved, the GDPR requires a written contract (a data processing agreement) where a "data controller" (ie you) uses a "data processor" (anyone that does anything with personal data on your behalf). Such contracts should clearly set out the responsibilities and liabilities of each party with respect to data protection.
- Take additional care if any data (particularly personal data) is likely to be stored outside the UK or European Economic Area (EEA) as legal standards of data protection may be lower elsewhere.

7. How long is long-term?

Accounting and tax

- Accounting and tax records for an ordinary limited company must be retained for at least six years after the end of the tax period they relate to.
- Self-employed sole traders or partnerships must keep their records for at least five years after the 31 January filing deadline.
- If you file your tax return late, or HM Revenue & Customs starts an investigation, you may need to keep your records longer.

Pay

- Pay records must be kept for a minimum of three years after the end of the tax year the earnings relate to.
- This includes sickness and sick pay records, and records relating to maternity pay, paternity pay and adoption pay.

VAT

- VAT records and documents must be kept for six years.

Contracts

- Contracts should usually be kept for six years after the contract ends, though contracts under seal (eg deeds) should be kept for 12 years.
- Legal claims under a contract cannot usually be brought outside these limitation periods, though there are exceptions.

Health and safety

- Health and safety records should be kept for at least three years.
- Records relating to hazardous substances may need to be kept longer. For example, asbestos records should be retained indefinitely,

Employers' liability insurance

- The requirement to retain your compulsory employers' liability insurance certificates for 40 years ended on 1 October 2008. You should still keep records of the insurance in case a claim is made.
- 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.

Six filing guidelines

Know what you have got

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

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.

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 or CD-ROM 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.

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.

Do not hold on to records longer than you need to

Dispose of old records safely

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

Signpost

- Download guidance on the tax records you need from HMRC.
- Find free and paid-for encryption software on Download.com.
- Find data protection guidance from the Information Commissioner's Office (0303 123 1113).

Expert quote

"In practice, confidential information is at its most vulnerable when you decide it is not needed any more. Make sure papers or files are shredded. You do not want to be responsible for pages of personal records turning up on a landfill site." - Richard Beevers, Beevers Consulting

July 2018

ACCA LEGAL NOTICE
This is a basic guide prepared by *ACCA UK*'s Technical Advisory Service for members and their clients. It should not be used as a definitive guide, since individual circumstances may vary. Specific advice should be obtained, where necessary.