

Personnel Skills

Aims

The aim of this course is to equip candidates with the necessary underpinning knowledge to work effectively within a personnel or HR environment in a supporting or administrative role.

It provides an introduction to Personnel Management and progression from this course could include studying for a CIPD qualification

Objectives

By the end of this course the candidate will be able to:

- Understand the importance of maintaining accurate personnel records
- Identify the main legal requirements of data protection and use of data
- Locate sources of further information and keep abreast of legislation
- Assist in conducting an effective recruitment and selection process
- Contribute to an effective induction process
- Appreciate the concept of self-development, and incorporate a plan of action to identify and act upon strengths and weaknesses
- State the difference between disciplinary, capability and grievance procedures
- Understand basic employment legislation including health & safety, equal opportunities and diversity

Certificate in Personnel Skills

Unit One

Records, Systems and Information Technology

Initiating and Maintaining Accurate Records

In this first module of the 'Certificate in Personnel Skills' course, you will be looking at the importance of initiating and maintaining accurate Personnel Records.

Personnel records are needed because:

- They comply with legal requirement
- They keep note of contractual agreements and/or arrangements between employer and employee
- They provide contact and ongoing details concerning employees
- They provide the organisation with information on which to make decisions (e.g. appraisal notes for promotion; qualifications to confirm suitability for posts etc.)

1. Compliance with Legal Requirements

All employers have a legal duty to:

- Keep records to safeguard themselves from claims that employees have been discriminated against, or unfairly dismissed (*Employment Protection Rights*).
- Keep records because government departments (for example, Inland Revenue) can ask for details such as: how many people are employed, how long they have been in your employment, how much they are paid, and how many hours per week they work.

- Keep records of any accidents, exposure to hazardous substances, and/or training provided to employees (*Health & Safety Legislation*). Employers have a duty to show responsibility for management of health and safety matters.

2. Contractual Agreement and Arrangements

If an Agreement is written down it is not only clearer for all parties to understand, but also easier to insist that parties adhere to it.

It is a legal requirement to provide written particulars of employment, but it is also good practice for an employer to provide them. If all parties are aware of what is expected from them, fewer problems or misunderstandings may occur. In any case, records will need to be referred to if a problem or dispute does occur.

Clear contractual agreements can provide evidence for defence if, for example, a claim is made via an employment tribunal.

3. Contact Details

Keeping contact details for each employee may seem one of the most obvious reasons for initiating and maintaining accurate personnel records – but let's consider *why* keeping accurate details are so important:

- People need to get paid! *An incorrect address may mean a lost cheque.*
- Contacting people at short notice to provide temporary cover during staff absence or to cover shifts at times of need. *Lack of up to date contact numbers makes this task very difficult.*
- Contacting family or next of kin if staff suffer a medical emergency whilst at work. *As above – but lack of correct or up-to-date information could be disastrous in this case.*

ACTIVITY 1: What other problems do you think might arise from incomplete or inaccurate contact information being held on file? Write a brief summary.

4. Providing Information

How would you assess staff turnover? Where would you turn for facts and figures to evidence your equal opportunities policy? Personnel records are able to record the detail that is required to help the business run overall, and assist major decision-makers in assimilating the information available.

Manual and Computerised Systems

Records can be on paper or card, written or typed. These are manual records (i.e. 'by hand').

Application forms, CVs, copies of Qualification Certificates and hand-written or word-processed letters are all received by the Personnel Department and either filed, or recorded and returned, or (in the case of some application forms, and letters) discarded (usually by shredding) when no longer required.

Mention computerised records and many people will think first of databases. Typically the information required for a database may take some time to input, but once the task is complete, there are many varied tasks that can be performed to track and analyse the data, making the personnel function easier.

For example, the database can be interrogated to answer questions such as:

- Has anyone not yet received Induction Training?
- How many employees can operate a certain machine/ have a specific qualification?
- Which employees fall within a particular salary band?

This is where you can provide some of the information that was mentioned in part 4 above.

Computers make analysis of management data much more efficient. The information available should be relevant, meaningful and help the decision maker. For example, knowledge that a senior manager is due to retire next spring would allow for a replacement to be found in time, as well as making pension or other arrangements for the manager who is leaving. Providing valuable information such as this in good time makes the personnel practitioner a most useful member of the organisation.

So, whilst both manual and computerised records clearly have their own merits (for example handwritten notes from a prospective employee can give an indication of the candidate's literacy – and the company may even use a graphologist to analyse the candidate's handwriting for personality traits), other benefits to Personnel of using computer (rather than manual) records include:

- Monitoring and completion of administrative tasks is easier by computer (anyone can pick up a task that someone may have previously started)
- Using a database or spreadsheet package can mean that much time is saved in what would otherwise have been a laborious manual task; with computerised calculations the margin for mathematical error is also reduced (provided the information is accurately input to start with)
- Details can be used more than once and shared between tasks e.g. the mailmerged letter sent out with an application form can be stored and letters then sent to candidates shortlisted for interview. Likewise the shortlisted candidates can be sent a mailmerged acceptance or rejection letter at the end of the interview stage without the sender having to duplicate names and addresses all over again.

We have mentioned the database above as an example of the Computerised Record section. However, documents such as Qualification Certificates or change of status proof (e.g. Marriage Certificate – for purposes of pension rights, for example) can be scanned into computers and their image kept on file. These are another example of a computerised record – it means that you can access the information at the touch of a button from your PC rather than retrieving what might be a dog-eared photocopy from a cabinet, if still performing manual filing of documents.

As well as being quicker and neater to use, the added advantage of a computerised record is the reduction in paperwork and physical storage space necessary. Indexing of documents by computer also makes the task of locating files much easier – and a task that everyone in the department can perform if required (and shown how!)

ACTIVITY 2: Can you think of five other example of documentation that could be scanned?

IT Software and Application in Personnel

Sometimes we might want to use a software programme that does not necessarily benefit us i.e. does not promote better business performance. For example, wanting the latest communication technology or faster access to the Internet – simply because it looks good! Cost is involved in identification of suitable IT software, of course, but the main consideration must also be whether it does the job we require it to do. In other words, we must consider “What do we need?” as opposed to “What do we want?”

Do you need software that allows speedy word processing? Software to produce organisational structure charts? Or graphics and colour printing?

To help you decide what the capabilities of your computer should be, consider what you will be using it for.

As an example:

Does your computer need to produce timely information? That is, for instance, if your computer were to flag up that an employee had been absent for an excessive number of days without a doctor’s certificate, it might trigger a letter from personnel to that person. So – do you need this facility on your computer, or do you simply want it?

You may want it (or even think you need it) but bear in mind the implications of having it. This will mean that attendance records have to be input first by someone – and if you have no-one available to do this on a daily basis, the information may be out of date or irrelevant by the time the situation comes to light anyway. If it won’t automatically promote better business performance under these circumstances (i.e. there is no-one to actually initiate or maintain those particular records) is there any point in having it? You may need to use other practical examples such as the one above when considering other requirements for the software used in personnel computers – but also there are other factors to consider in use of computers generally:

Accuracy

As long as the raw data has been accurately put onto the computer, it should remain accurate – but this very much depends on the operator or (in the case of complex calculations, for example) the programmer. Once input, dependent on the capabilities of the software package used, the data can then be asked to perform calculations relevant to personnel function, such as calculating employees' ages (continuously and automatically updating this information) from the date of birth and current date, and such data can then be electronically transferred and used elsewhere in the company e.g. by pensions department in pension calculations, or salaries, for wages increase.

Printing Capabilities

You will need to give thought not just to the software (i.e. programs for the PC – variety of fonts, selection of graphics) but also to the hardware required for printing (i.e. the physical components – e.g. size of printer, perhaps to fit the work space available or to accommodate the different size and types of paper used in printing).

Access to Information

How easy is it for relevant staff to access the information on your computer? Do you need restricted access only (see Data Protection below) – in which case the use of passwords, or locking the computer and/ or the office at night might suffice. Will the computer be networked elsewhere within the company? If so, you need to safeguard against any unauthorised access.

Security

This does not mean just allocating a password at Login to your PC. Security threats include:

- Computer viruses – many people have already experienced or heard about the MS Worm Blaster virus which attached itself to emails and caused the MS system to close down in one form or another
- Fire
- Computer failure ('crash') for whatever reason

- Accidental disruption (e.g. spilling a drink over the keyboard)
- Even deliberate disruption to the computer system (i.e. sabotage).

To secure your files long term, you should regularly back them up. Back-ups are particularly useful if your data is corrupted by a computer virus – you can refer back to your last (unaffected) back-up and at least salvage the majority of your work/ files.

In safeguard against fire or deliberate disruption you should keep these back-up disks in a fireproof safe or at least under lock and key.

Use a firewall (software that can be installed to protect your data from any outside party accessing it).

ACTIVITY 3: What would happen to your personnel records if someone broke into the office overnight and deliberately erased them all? Do you have the necessary protection against this, or indeed any back-up plan should it ever happen? Detail your answer.

Data Protection Act 1998

Any personal data that is held in a 'relevant filing system' is covered by the Data Protection Act 1998. This includes manual filing systems, emails, computer records, even taped telephone conversations. (You may recall being advised by an answerphone that 'phone calls may be recorded ...etc.' when you are waiting for a company, such as an Insurance broker, to answer).

Your company needs to be registered with the Information Commissioner if you intend to hold, obtain, record or process any personal data. As a personnel practitioner, you should keep abreast of any changes in the Data Protection Act. In order to do this, you might need or wish to obtain a recent copy of the 'Code of Practice', which is available from:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Or available from the web site at: www.informationcommissioner.gov.uk

In general, the following data protection principles apply:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless
 - a. at least one condition in Schedule 2 is met and
 - b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

** Conditions cover consent and legitimate interests as well as a number of specific conditions such as the administration of justice. Sensitive data may be kept for ethnic monitoring purposes. Data classed as 'sensitive' includes any reference to racial or ethnic origin, religion, physical or mental health condition, trade union membership, sexual orientation, or political opinion.*

Using such data requires the explicit consent of the person concerned unless the information is already made public (or if it is used for ethnic monitoring purposes e.g. to establish/promote Equal Opportunities in the workplace). Explicit means seeking permission from that individual to use the data. If you have permission to use data for one purpose only, you cannot use it for another purpose without seeking explicit permission again.

Under the Data Protection Act 1998 it is actually an offence to hold personal data without being registered to do so. Also anyone whose data you have collected (in this case, your employees) has a right to 'subject access' – that is, they can see what information you hold about them and ask the purpose for holding that information.

A personnel practitioner must be very careful not to disclose confidential information being held about any employee to an outsider whether accidentally, deliberately or through simple bad judgement e.g. not

checking the identity of a telephone caller claiming to be from another company seeking a reference for an employee.

It is better to check and get back to the caller e.g. take their name and ring through to the main switchboard of the company to check that the person is calling from there. If the ID of a caller cannot be easily verified confidential information should not be passed over the phone – ask the company to write or fax their request, or hand a letter of reference to the employee who needs it. Another employer making a bona fide request will respect your concerns over this issue and should be impressed that you are protecting your own employee (even if it does make their job harder!)

Your own friends, not just ‘outsiders’ may see the personnel department as the fount of all knowledge and some may even try to inadvertently abuse your position of trust. For instance, someone may ask for the home phone number of another member of staff: It is better to take the caller’s number and tell them you will have the staff member ring them back when you have spoken with them direct, or at least first seek permission from the member of staff to release their phone number to someone else.

Email and Use of the Internet within Personnel

Does your Personnel Department have a policy or guidelines on the use of the Internet and/or emails within your organisation? If so, are you fully acquainted with the policy – and are your staff regularly reminded of its content? If not, should you be preparing a policy – and what would you include?

Professional use of the Internet is a quick and easy method of research (for everything from hotels and travel bookings, to competitors’ plans and annual meetings); private use of the Internet is usually for social or non-work interests and the use (or misuse) of this facility at work can constitute a disciplinary matter if employees are aware that it contradicts company policy.

So, for example, many organisations state quite clearly that downloading (or even accessing) pornographic material is a disciplinary matter. But

how will the company monitor what is being used on their computer systems? Whilst the employer has a right to know if their system is being misused, the employee has a right to a certain amount of privacy. These issues have to be taken into account when developing a policy for use at work.

Regarding use of email, employees should remember that sending an email on the company computer system is almost equivalent to sending a letter on company letterhead, therefore the facility should be used carefully and with good intentions only.

Do not send an email from anyone else's email address unless making it perfectly clear to the recipient that you are not the person named on the system e.g. "This is Mr Jones replying to your email on behalf of Mr Smith."

Confidential information (for example, salary details for a job offer) is best not sent via email as it can be intercepted, go to the wrong address, get copied erroneously to all recipients in your address book etc.! Better to send a Private & Confidential letter unless you can send an encrypted email and check that the person concerned is the only one who will be able to open it.

Sending an email to lots of recipients at once means that many people on your address list will have their address seen by others – including, perhaps, people they do not know; email addresses are another form of personal data and as such are covered by the principles of the Data Protection Act 1998 too. Therefore using a personal email address list unwisely could lead to a breach of the individual's privacy (like giving out their home address or telephone number).

It need only apply if sending emails to home addresses as work email addresses can be found in the internal phone directory, or are generally known, anyway. So check whether you need to send any 'home address' emails at all – and if you do, can you set up 'Groups' so that only certain sectors of people (i.e. those who work in same department, or all who know each other's personal email addresses already) receive the same email at the same time.

ACTIVITY 4. What would you do if a colleague asked you for their friends' phone number from the Personnel File?

What would you do if you found that someone had given another person your home email address?