

P5 – Employee Contacts

Contracts are a set of rules or stipulations that employees must agree to in order to work for an organisation. Employers are legally required to provide a contract in order to hire employees, and must also explain which parts are legally binding, rather than just an informal agreement between the employer and employee.

They primarily help with legal issues. For example, if an employee breaks the contract, the company has every right to fire them, and as the employee signed the contract, they cannot argue about it. This stops organisations being dragged into court cases, saving them money and resources.

Most contracts will cover the employees' rights (working hours, pay, available resources, etc.), and also rules or policies they must follow. For example, a contract might say an employee is entitled to a certain amount of pay per hour, or that aggression against other staff members is grounds for being fired.

A contract will also cover the employee's duties and responsibilities. This is like a more in-depth version of a job description.

Each of the stipulations in a contract is called a 'term', much like terms & conditions. A contract doesn't necessarily have to be written down and signed – just accepting a job offer is a form of contract.

Free-lance or one-off jobs do not have employment contracts. For example, if somebody agrees to edit a video for somebody, they are instead under a 'contract to provide a service' – that is, complete the work to a standard and within a deadline agreed between the two parties.

Contracts are not just for the employee – they also cover the employer's responsibilities, such as providing things like training, resources necessary to do the job, and a method of raising any concerns an employee might have.

An important aspect of a contract for any employee working with an IT system is security. The contract will generally instruct the employee to follow an IT security policy, which will cover working procedures to minimise risk to the system. This will include things like what the system can and can't be used for, as well as how to deal with problems that may arise.

This ensures that employees do not cause risk or damage to the system, unintentionally or otherwise. An example of this is that the NHS does not allow staff to use USB sticks to transfer data between work and home computers, as it is possible the home PC could infect the USB stick with a virus and crash the NHS system.

Similarly, any organisation that deals with sensitive data must have all employees follow the Data Protection Act. This will be mentioned in either the contract, or the contract will refer to the policy.