Information security

Confidentiality

Who can see the information?

In a business, only some members of staff are chosen to be able to access certain parts of information a business stores, and with that also only a few people in the company are able to update and change the information (if necessary). So if (for example) a business were to keep a database containing staff details and personal information, this info should be kept secure from any unwanted access. Consequences that could happen if information like staff’s personal details were to be accessed by an unwanted user is that the personal details could be used for identity theft resulting in many problems for the company.

Who can update the information?

A business manager in a company would have to decide who exactly can view and update information stored in the company, and would have to make sure to do backups so that the information won’t get lost. For example, only certain staff will have access to information stored within a company and would update information about a staff, such as if an employee has had a birthday, their age would have to be changed, and so this information would have to be backed up and stored securely.

For how long is the information to be stored?

In every business information based on staff are kept stored within the company. This could be addresses, DOB, and bank details. After a certain amount of years (if the employee has left the company) this information would then have to be destroyed as they are no longer with the company. In a school every student’s details are recorded and are accessed and updated by staffs that is able to. If a student were to leave the school their information would still be kept in that school until after 5-6 years since they’ve left. After the time to keep a student’s record is up, the information must be destroyed.

What information is stored?
Information stored can be personal details of all staff including contact information (name, address, phone numbers), references and bank details.
What systems are available to store the information?

Systems storing personal information such as bank details credit records or medical records must be accurate and managed in a confidential manner. Companies can use databases in order to keep record of customer information such as personal details, for example if they were to sign up for a loyalty card for a supermarket, their information would need to be recorded into a database so they are able to use their card and gain points.

How often the information must be reviewed for currency?

If an employee were to move house then their information would have to be changed so that any letters, checks or anything from the company they work in would have their right address in which they’d have to send these things to. The same goes for bank details. If an employee’s debit card that is issued to the company so they can receive their income were to be stolen, and if they had gotten that card replaced, this information would need to be updated so that no problems would happen, and that their employee would receive their income from that company. Also a member of staff would have to review regularly staffs information checking whether it has been updated or not, so that all information can be accurate.

Integrity and completeness of data

Having incorrect data can cause problems

The integrity and completeness of data is serious, for example, if an organisation were to have incorrect data (such as contact and personal details and also bank details) of an employee, this can cause some damage as this means that if the data is incorrect, then the employee would not be receiving their payments from the company (and the money could be going to someone else), or the employee would not be able to receive letters from the organisation they work in as they have not got the correct or complete data on the employee. Therefore it is always essential that information should be complete and correct.

Get people to check
When it comes to storing data, it must always be correct. If a hospital were to store incorrect data about a patient it could lead to some unwanted consequences. Staff in a business who fill in data for either other employees or customers must make sure that all information is accuracy, so for example if an employee’s bank details were wrong, that person wouldn’t be receiving money, therefore asking another member of staff to check the data for accuracy is necessary, and updating the information from time to time should be done, just to make sure that everything is correct.
Access to data
In a business, it should be essential that they check who has access to data in a company as they control the availability of the data they have access to, and it is important to review regularly exactly who has access to data within the company, as they might not be in need of it as they haven’t been using it regularly or if the data that is being accessed is being used negatively for wrong reasons. This can be managed by having staff review who has access to what, and if (for example) an employee were to gain access to data, and have gone over the time limit, the staff controlling who can have access can revoke them from access as they have gone over time limit, and also access can be driven by a legal protocol, and so this is handled by having a number of user rights, as well as password control.