# Answers to Component 3 activity sheets

### Activity sheet 3.1: How to use an ad hoc network

1. An ad hoc network is a network that enables devices to connect to each other directly, for example using Bluetooth.
2. PAN, open-Wi-Fi, personal hotspot.
3. Trains, hotels, client offices, cafes.
4. Search for the hotspot SSID (service set identifier) in their Wi-Fi settings. Enter any required security, for example Wi-Fi password. Agree to any terms and conditions (if any). Join the network.
5. For example, by Bluetooth. Client selects file and sends by Bluetooth. Consultant’s device detects possible incoming file. Consultant’s device pairs with client’s device. File is transmitted.
6. Benefits – more and faster communications, less need for network management devices, for example routers.

Drawbacks – less control over networks and data transferred. Some ad hoc networks have poor security, increasing risk of data loss/hacking.

1. Lack of security credentials, loss of signal. Network may not have connectivity outside of itself, for example to internet, so unable to transfer data to/from internet.

### Activity sheet 3.2: Using cloud storage

1. **a.** Because the service only works if there is an internet connection – this is how data is transferred to and from the cloud service.

The file is stored on his laptop until there is an internet connection – the file will then be synchronised when the connection is established.

The file in the cloud will also be deleted.

They can increase the amount of storage available to them – this may cost extra.

1. **a.** Misha can put the files onto a USB drive.

Misha could email the file as an attachment to an email message.

She could ask a colleague to email it to her. If nobody else at the office has access to the file, she will have to visit the office herself.

Misha could manually upload documents that she has edited, or she could use a local service that synchronises files between the local area network and her laptop.

### Activity sheet 3.3: Working with cloud computing

1. **a.** Web browser.

The web browser connects to the cloud computing service. The browser then downloads the data needed to run the word processor inside the browser.

The web browser will upload any edits made in real time.

It would take a long time for the web browser to download the application. Each edit Raj makes would take a long time for the web browser to upload. The service would freeze and then unfreeze.

Raj would not be able to use the cloud computing service. He may be forced to use outdated documents on his computer.

1. **a.** Misha’s laptop would need a word-processing application installed on it. It then needs   
   to be possible for documents to be downloaded to the laptop and uploaded from it once completed.

Data is stored on the laptop, so if it is damaged she may lose her work. The laptop could be dropped therefore destroying the internal storage device.

Benefit: Misha can work in places where there is no internet connection.

Drawback: Misha will need to make sure that her work is backed up.

### Activity sheet 3.4: The paperless school

### Learners’ own response.

### Activity sheet 3.5: Using cloud and traditional computing together

1. Learners’ own interpretation (see PPT 3.5 for an example).
2. Data is uploaded to the cloud each time she makes an edit to the document. This is then synchronised to the other devices each time they connect to the service.
3. The file will be deleted across all her devices. Only a back up would preserve a copy of the file. Laura will lose her work if it is not backed up. A back up is usually made on another device so Laura could easily retrieve this.
4. She could configure it so that copies of files on the cloud are not stored on the tablet. If she needs to work on a file, it can be downloaded but all other files are not stored on the tablet.

### Activity sheet 3.6: Choosing a cloud service

### Learners’ own response.

### Activity sheet 3.7: Should we use a cloud-based provider?

1. To update the service; to improve the service by adding or removing features; to replace critical hardware, for example a server. They may also need to improve the security that they offer to its users.
2. Yes, if they need to use the service then. This is likely, given the time zone difference between New York and England.
3. Yes they should. Downtime causes problems for their users and the users might go elsewhere if there is too much downtime. The ability to have no downtime is a major ‘selling point’ for a cloud computing provider.
4. They know how much they are going to pay each month.
5. The provider could increase their fees, and if Allan’s Travel Services do not change provider,   
   it means their costs of doing business will increase.

### Activity sheet 3.8: Collaborative working at Jackson and Jackson

#### Scenario 1

1. Video conferencing or teleconferencing.
2. This will enable both partners to answer the client’s questions. A drawback though is the time difference.

#### Scenario 2

1. Use collaborative technology to enable Andrew to review the draft and make comments and changes (Tracked changes).
2. Riley can then read the comments, and any changes made by Andrew can either be accepted or rejected by Riley.

#### Scenario 3

1. Riley can email the questions to Andrew.
2. Andrew can work on them while Riley is asleep. Riley can then read Andrew’s responses the next morning.

#### Scenario 4

1. Riley could phone Andrew but the signal might cut out if the train enters a tunnel. Instead, they could use an instant messaging service.
2. This would also drop out in the tunnels but at least one of them can be typing while waiting for the service to reconnect.

#### Scenario 5

1. Collaborative shared document.
2. Similar to Scenario 2, but the document should be set to read only when the other partner is using it.

### Activity sheet 3.9: Review of collaborative working activity

### Learners’ own response.

### Activity sheet 3.10: Using diary management software

#### Scenario 1

Invite all four people. Enable participants to suggest alternative dates. Do not allow them to decline the meeting.

#### Scenario 2

Schedule the meeting and place it into participants’ diaries. Also set up a reminder to attend the meeting; for example one for the end of the previous working day and one for one hour before the meeting starts.

#### Scenario 3

Set up each meeting and the lunch break in Terry’s diary. Set a reminder five minutes before each interview. Set Terry’s status to either Do Not Disturb or Out of Office until 5.30 p.m. (whichever one is available on the diary management system).

### Activity sheet 3.11: Choosing communication channels and technologies

1. **a.** Smartphone app: public channel. Users download the app. They can then enter a number corresponding to the display item to view information about the item.

**b.** Digital display board above each exhibit such as a large TV screen or projector screen. Display will be easier to see because of its position.

**c.** Digital audio guide. Users select an exhibit using a keypad and information is read aloud and listened to through headphones.

1. Private: between one person and another – usually to exchange personal information.

Public: one person communicating with many people – usually non-confidential information.

1. **a.** Reminders of opening and closing times.

**b.** Information about special events.

**c.** Safety information, for example warning of a fire drill.

1. **a.** Confirmation of a customer’s booking.

**b.** Confirmation of address for posting tickets.

**c.** Confirmation of payment details, for example bank card details held on file.

### Activity sheet 3.12: How can we make our website accessible and inclusive?

1. Remove references to males only (he, his) – the information applies to all drivers regardless of gender. Mankind could be changed to humankind.
2. Learners’ own responses. Examples of sites that are inclusive may include ones where content can be displayed clearly on different devices (for example, mobile phone and desktop PC), where visually impaired users can obtain the same information from a visual object as a sighted person; where there is a good contrast between the font and background (to make   
   it easier for those with dyslexia to read), etc. Sites that are less inclusive may have been originally produced some time ago and have not been updated. Examples might include small, locally based organisations such as community groups or sole-trader businesses.

### Activity sheet 3.13: ZZ Game Developers – the impact of new technology

1. Cost 1: Cost of purchasing the devices. The devices will each cost a sum of money to buy. This is a one-off cost at the start of the product’s life.

Cost 2: Training. ZZ Game Developers may have to pay for training to enable the staff to be able to use the devices fully.

Possible other costs include: cost of installing software (licences), costs of subscribing to security software (ongoing costs), repair and replacement costs (in the event of loss, damage or wear and tear), insurance and extended warranty costs.

1. Benefit 1: Staff can work remotely. Staff can work when not in the office – this will help to make them more productive by being able to complete more tasks during the working day.

Benefit 2: Less office space is needed for equipment. If the laptops replace existing desktop PCs, then they will take up less space in the office. Desks could be made smaller so, in time, less office space is needed – this will help to reduce costs.

1. **a.** Staff may use the smartphones for personal use. This will reduce productivity.

**b.** The devices are portable so are more likely to be lost or stolen than existing office equipment – this could be a security risk because of the data they might contain.

1. **a.** Orders can be placed at the customers’ convenience, not just at the convenience of the business, so more orders could be taken, for example late at night.

**b.** Orders could potentially come from anywhere in the world, expanding the customer base and so, hopefully, increasing the number of purchases made.

1. **a.** Customers can order at their own convenience – no need to travel to a physical store.

**b.** Some customers work during the day and so may only be able to make purchases in the evenings when a physical store would be closed.

### Activity sheet 3.14: ZZ Game Developers – how technology affects business activities

1. • Computer (with sufficient processing power and a large enough screen, for example a medium-sized laptop or larger).

* Video camera (for example an inbuilt webcam).
* Microphone and speakers (ideally a dedicated microphone with headphones attached to prevent feedback distortion between a loudspeaker and the microphone).
* Software – many video conferencing facilities operate though a web browser but sometimes specialist software is needed.
* A fast internet connection (2G or 3G mobile internet is unlikely to be fast enough).

1. **a.** Meetings are less expensive – no need to pay the travel costs of those attending.

**b.** More meetings can take place – each meeting takes less time to arrange (for example minimal travelling time needed). There is less travel time so employees can be getting on with other tasks.

1. **a.** Quality of technology can sometimes mean that meetings are not effective, for example some participants may struggle to hear others.

**b.** Less opportunity for all participants to see each other – less face-to-face interaction, so the quality of communication may suffer. It may not encourage a team spirit.

1. **a.** Fewer resources needed than video conferencing – cheaper to organise and operate.

**b.** Can take place ‘on the fly’ – a developer can post a question and whoever is also on the system can give a reply.

1. **a.** Rely on text only – developers need to be able to state in words exactly what they mean, otherwise communication may not be effective.

**b.** Depends on an active connection between system users, for example internet connection.

1. **a.** Assistive technology means that people with specific needs can use technology to fully engage with co-workers and customers.

**b.** Technology enables more home workers (including people with domestic commitments who are unable to travel to an office) to be employed.

1. **a.** Fewer resources needed in the office, for example desks, chairs, computers, etc. Smaller office = reduced business costs.

**b.** A wider range of employees can be employed, including those who have domestic commitments or are unable to or prefer not to travel.

1. **a.** Might be harder to monitor their work – are remote workers at work when they should be?

**b.** Requires technology that enables remote workers to exchange data with the office – potential for increased financial costs, disruption caused by failure of equipment, and security risks, as confidential data is potentially being stored in a non-secure location   
(i.e. the employee’s own home).

**Activity sheet 3.15: Could you cope with working remotely with technology?**

Learners’ own response.

# Activity sheet 3.16: Building skills for assessment activity

#### Using cloud systems

1. Tethering is where a smartphone acts as an access point, allowing other devices to connect   
   to it using wired or wireless connectivity, in order to share its mobile broadband connection to the internet.
2. Open Wi-Fi connections may not be secure. Lots of users may be able to access these which means that the data on the network may be intercepted.
3. The signal may be poor or intermittent. The data transfer range may also be limited. The devices can only connect if they are in the same room.
4. Emilia will pair her device with the client device. Once the connection has been established, Emilia will be able to send a file transfer request to the client device. Once accepted, the files will then be transmitted.
5. Benefits include:
6. You are able to move around easily and therefore you can move somewhere to get a   
   better signal
7. Different people can quickly join the network to view the videos/files when needed.

Drawbacks include:

1. The signal may not be stable and therefore there may be breaks in the video/sound
2. The connection may not be secure and therefore sensitive communication can be intercepted.

#### Collaborative working

1. Workflow is when only one person can work on the document at a particular time. The person who currently has access will have edit access so that they can make changes. Everybody else will have read access so that they cannot make changes while another person within the team is making changes.
2. Karen can see a log of what has been changed and who has changed it is kept. Therefore,   
   she can see what changes have been made and then either agree with them or disagree with them. If she disagrees with them, then the document can be rolled back, which will delete the changes she disagrees with.
3. **Manage the tasks that each team member must perform:**
4. A to-do list to list and allocate work to different members of the team
5. A message board to give updates or news to the team about the work being completed.

**Organise and monitor deadlines:**

1. A schedule to show key dates and deadlines.

#### The impact of technologies

1. Benefits:
2. They may be cheaper than desktop PCs
3. They are more portable so the business can move them between work and home.
4. Drawbacks:
5. They are easier to get lost or stolen
6. As they are portable, they may get damaged easily
7. The screen size may be smaller.

### Activity sheet 3.17: What happens after an attack?

1. Damage to reputation: patients may lose confidence in the surgery and leave; possible legal consequences if data protection legislation is deemed to have been broken.
2. Loss of client confidence; loss of customers and income; may have to pay compensation to the client; financially potentially very expensive for PCB Services.
3. **a.** He will suffer financial loss. Will the files be released? The attacker may ask for   
   more money.

**b.** His files will probably not be released. His computer system may remain unusable.

1. Major loss of income from customers unable to buy from the store. Customers will most likely shop elsewhere resulting in loss of income now and in the future, as some customers will   
   not return.
2. **a.** Loss of income; damage to reputation; possible legal consequences.

**b.** Customers may be potential victims of identity theft or fraud as their personal details are used to set up fake accounts or make purchases. Customers will face the inconvenience   
of securing their other online accounts, for example those that use some or all of the same security information.

### Activity sheet 3.18: Is this a threat?

1. **a.** Social engineering.

**b.** User’s security credentials, for example username and password.

**c.** Ignore it. Report it to the bank using the contact information on the bank’s own website. Delete the text message.

1. **a.** Phishing.

**b.** Username and password. Most such attackers work on the principle that the respondent uses weak security, for example the same username and password on other accounts,   
so these will be used to try to hack into other accounts.

**c.** Report the email as a scam and delete it. Any appropriate reasons accepted.

1. **a.** Not genuine. Too many errors, including spelling errors. The hyperlink is clearly not for a legitimate business as it does not match any known organisation. It does not greet the person by name.

**b.** Report the email as a scam and delete it. Any appropriate reasons accepted.

### Activity sheet 3.19: Dealing with internal threats

#### Scenario 1

* 1. Visiting untrustworthy websites. Malware may get released onto the computers.
  2. Prevent users from visiting some sites. Consider using an allowed list of approved sites. These could be set up on the firewall.

#### Scenario 2

* 1. Potential for viruses and other spyware to be downloaded.
  2. Ensure anti-virus systems are up to date and working correctly.

#### Scenario 3

* 1. Disclosure of data, for example staff taking unauthorised files home and accidentally or deliberately sharing them.
  2. Consider disabling this facility so memory sticks are not recognised when plugged in, or using a cloud computing solution where users can view and edit documents online but not download them.

#### Scenario 4

* 1. Staff may steal or leak information, for example by taking it with them to a competitor.
  2. Consider any measure to limit ability of staff to remove files such as file access rights, for example any of the above measures.

### Activity sheet 3.20: Improving security at StreamSongs

1. **a.** External access to systems, copying files, stealing equipment.

**b.** Avoid stealing information.

**c.** Staff with access may allow into the room those without access, for example by holding door open for others. Swipe cards can also be lost and picked up by other people.

1. **a.** Deter theft of equipment.

**b.** Avoid stealing or leaking information.

**c.** Only records actions taking place; does not prevent them.

1. **a.** Disclosure of data.

**b.** Staff less likely to be able to override security controls.

**c.** Staff need access to their smartphone; some organisations screen premises to limit smartphone use.

1. **a.** Stealing or leaking information.

**b.** Staff only have access to limited information, relevant to their job role.

**c.** Does not prevent staff from leaking information they have access to; this includes senior staff with access to more information.

1. **a.** Shoulder surfing.

**b.** Disclosure of data.

**c.** Can the system be fooled by using a photograph of the user’s face?

### Activity sheet 3.21: Using a firewall and anti-virus software

1. **a.** A firewall limits the transfer of traffic into and out of a network based on the rules in place but does not scan it for viruses. Anti-virus software scans any traffic for viruses, regardless of origin.

**b.** A firewall should only accept incoming traffic that has been requested by the user, for example the files needed to view a webpage in response to the user clicking a link to view the page. It should also only allow access to traffic that does not break the rules in place.

1. **a.** Do not allow. It could be malware. Check with an IT technician first if seriously considering accepting it.

**b.** Some trusted programs (for example a spreadsheet) may contain links to known and trusted external websites. The firewall can be configured to always allow such programs to exchange information with external websites.

1. Anti-virus software helps to keep the system virus-free. It is likely that without one a virus could affect the system.
2. **a.** New viruses appear all the time. Unless part of the virus code is contained in the library, the anti-virus software will not detect it.

**b.** Anti-virus software needs to be ‘always on’ – on some older systems this can use processing power that slows down the system, for example other programs take longer to load.

### Activity sheet 3.22: Device hardening at Jackson’s Solicitors

1. • Vulnerability: greater chance of viruses being installed.

* Action to correct: install or switch on the firewall.
* How the action will make the business less vulnerable to attack: such files will either be blocked or flagged to the user so that they can decide whether to allow.

1. • Vulnerability: viruses can be installed.

* Action to correct: install or switch on anti-virus software.
* How the action will make the business less vulnerable to attack: suspicious files can be automatically blocked or deleted.

1. • Vulnerability: operating system vulnerable to attack – malicious users can take control of the system.

* Action to correct: ensure operating system is updated. If the operating system is no longer supported by the manufacturer, then it should be replaced with an up-to-date one.
* How the action will make the business less vulnerable to attack: operating system less vulnerable to attack as it is likely to contain patches that prevent known attacks from being able to succeed.

1. • Vulnerability: files and their contents can be intercepted during online transfer and the contents read.

* Action to correct: use encryption software.
* How the action will make the business less vulnerable: files are encrypted during transfer and while stored on computer; less likely that unauthorised users can view them.

1. • Vulnerability: malicious programs can be installed.

* Action to correct: change access rights so that only authorised users (for example, IT administrators) can install programs.
* How the action will make the business less vulnerable: less likely that malicious software will be installed.

1. • Vulnerability: sensitive files can be copied by anyone.

* Action to correct: change access rights so that users can only view files relevant to their   
  job role.
* How the action will make the business less vulnerable: fewer staff can access fewer files.

### Activity sheet 3.23: Penetration testing

1. Authorised white hat hackers attempt to enter the system – playing the role of a malicious hacker. They are hacking for good reasons and report their findings to the organisation.
2. Ethical hacking – white hat – no intent to damage the system. Aim is to find vulnerabilities and close them.
3. White hat – see above.
4. **a.** 1. Authorisation to act.   
   2. Attempt to gain access and discover vulnerabilities and weaknesses.  
   3. Exploit any weaknesses (without disruption).  
   4. Document issues found.  
   5. Recommend security improvements.

**b.** Any appropriate description of each of the above stages

1. They should implement the recommendations but first they should ensure that the recommendations are technically possible and will not cost so much that they are not cost effective. It may be better in extreme cases to replace systems rather than patch them.

### Activity sheet 3.24: Producing a disaster recovery plan

**1.** and **2.**

Risks/effects/action to take:

* Loss of internet access/Unable to talk with clients or transfer files/Does Sharon have mobile internet access that can be used as a back up?
* Basement flooding/Damage to equipment/When she is away from home is the equipment secure from water damage, for example moved to higher floor level?
* Theft/Equipment may be stolen/Since the basement is easy to access from ground level, are entrances/exits secure? Is the room visible from the outside?

1. As a rule, customer personal data and sensitive business data (for example, financial records) should be backed up more frequently (for example, daily) and to a more secure location (e.g. encrypted cloud transfer/storage) than operational information (for example, operating system preferences).
2. Sharon’s system would probably need to be back up and running within a week of a major disaster – she mostly uses easy-to-obtain office computing equipment and if her files are correctly backed up she should be able to recover within days.
3. See above. It may be possible to use the services of an office rental business that also supplies equipment, but she should be able to source replacement equipment within a few days.

### Activity sheet 3.25: How secure are your passwords?

Learners’ own response.

### Activity sheet 3.26: Is the policy acceptable?

1. **a.** Not acceptable – any appropriate explanation. New draft: ‘Users must not install software onto their laptop without the permission of their supervisors’.

**b.** Not acceptable – any appropriate explanation. New draft: ‘Users, with the exception of approved IT staff, must not uninstall software’.

**c.** Not acceptable – any appropriate explanation. New draft: ‘Users’ software will update automatically. These settings can only be changed by an authorised IT officer’.

**d.** Not acceptable – any appropriate explanation. New draft: ‘Laptops will be audited by authorised IT staff. This can take place at any time and users must permit this to happen’.

1. Ensures that staff who do not follow procedures can face disciplinary action; ensures greater compliance with acceptable use.
2. What software can be installed; who can install it; when and how it can be updated; authorised modifications to system settings.

### Activity sheet 3.27: What to do after an attack

1. **a.** Hacking.

**b.** 4.

**c.** Has affected client files – important client.

**d.** Document storage.

**e.** Client must be informed as well as Data Protection authorities.

**f.** Secure systems.

1. **a.** Denial of service/DOS.

**b.** 5.

**c.** Systems are inoperable.

**d.** Website; possibly email as well.

**e.** Government/legal authorities – to see whether they are part of a larger attack.

**f.** None needed but the police should be informed, so they can assess the scale of the attack, and any other organisations affected.

1. **a.** Phishing.

**b.** 3.

**c.** Attack itself is relatively small but the method used suggests that the email systems  
are vulnerable.

**d.** Email.

**e.** No need to contact internal stakeholders but all staff need to be informed.

**f.** Need to review and update email account settings; lock all email accounts and require all staff to update passwords in order to unlock them.

1. **a.** Malware.

**b.** 5.

**c.** Potentially large financial consequences.

**d.** Any used by the Finance Officer.

**e.** Suppliers – bank must be contacted.

**f.** Immediate: isolate the computer and wipe the hard drive/reformat it/reinstall operating system to hopefully remove malware. Alternatively, isolate the equipment and have it investigated by authorities for evidence of how the crime was committed. Immediately contact bank and freeze accounts until security credentials are changed.

### Activity sheet 3.28: Building skills for assessment activity

1. **a.** Intellectual property is an idea that you invented that belongs to you, for example, an image that is copyrighted.
2. Ransomware is a form of malware, usually infecting unprotected digital systems, occurring when users open malicious email attachments.
3. Denial-of-service (DoS) attacks attack a remote computer by making it unable to respond to legitimate user requests.
4. Identity theft is when personal information about a person is stolen and an account is set up in their name.
5. Social engineering is the act of getting users to share sensitive information through a false pretext.
6. Phishing is a cyberattack that sends spam messages to try and trick people to reply with desired information.
7. Pharming is a cyberattack that uses malware to direct a user to a fake website that requests information.
8. Man-in-the-middle attacks are where the communication between two devices, for example a user and a web server, is intercepted and potentially tampered with.
9. Possible answers include:
10. Setting up weak passwords
11. Sharing passwords with others
12. Transferring data without adequate protection
13. Responding to a phishing email.
14. **a.** Locks could stop attackers getting physical access to data and devices.
15. User access rights can stop users/groups of users accessing data that they are not authorised to access.
16. Biometrics can be used to correctly authenticate a user.
17. Two-factor authentication will strength the security as it requires the users to know and have something.
18. Firewalls would stop unauthorised access to data.
19. Anti-virus software will stop viruses from being installed that could be used to corrupt data.
20. Data encryption will stop data from being read if accessed. However, it will not actually stop the data being accessed.
21. An organisation can employ an ethical hacker to try and break the security that is in place. They would try to hack into the network to check how secure the network is. If they managed to gain access, they will then provide a report to the organisation so that they can improve their security.
22. An Acceptable Use Policy (AUP) will improve the security as it sets the behaviour that is expected of its users. For example, it may state that users cannot share their passwords or state the password complexity rules. It may also state certain websites that users cannot access, for example, those that are more likely to contain viruses. However, an AUP is only a policy and is not enforced by law.
23. This could be any of the following:

**i.** Investigate the attack.

* + 1. Respond to the attack.
    2. Manage the attack.
    3. Recover from the attack.
    4. Analyse the attack to see how it can be avoided in the future.

### Activity sheet 3.29: Sharing data at Banstall Buses

1. The app takes the user’s location from GPS data, then searches for the nearest bus stop using a map containing the locations of all the bus stops. The app then requests details of the next available bus arriving at that stop – this is either taken from the bus timetables (planned arrival times) or from GPS trackers on each bus (giving estimated arrival time based on bus location and distance from the stop).
2. **a.** Provide details of other nearest bus-related services, for example nearest bus depot or nearest ticket office.

**b.** Provide information about other local services, for example supermarkets and banks.

1. They could use this to identify the most popular routes. This could help to make timetable changes by expanding popular services or cutting back less popular routes. More buses could be added to busy routes, possibly by being diverted from less busy routes.
2. **a.** Is an excessive amount of data being shared? For example, is personally identifiable data being shared, such as names, addresses?

**b.** Are the other organisations using the data for specified purposes only? Is it being used to send adverts that are not approved by the bus company?

**c.** Can the customers opt out of receiving the adverts? Do they have a choice over how their data is being used?

# Activity sheet 3.30: How green is your school or college?

# Learners’ own response.

### Activity sheet 3.31: Equal access to information and services

1. Nobody has faster or better access than anyone else. For example, everyone being able to access revision sites on the internet gives everyone an equal opportunity to perform at their best in an exam.
2. **a.** Some pupils may do less well at school – for example, being less able to complete research-based homework activities.

**b.** Some pupils may not have access to social media and so may miss out on opportunities to connect with friends, for example, during the school holidays.

1. **a.** The business will benefit from being able to send data to customers more easily – for example, videos of how products work. This can improve the level of customer service making it more likely that customers will buy from them.

**b.** The business will be able to have some of its workers work from home – the performance of these workers will not be slowed down by having a slow internet connection to the main office.

1. **a.** Customers will face delays on the website when placing orders. This will frustrate them and some will buy from other businesses with faster connection speeds.

**b.** The business may not be able to benefit from having some of its workers work from home. It may have to have larger offices as a result – costing it more money.

1. **a.** Greater inclusivity – everyone will have access to the same services: for example, the ability to book online appointments at a GP surgery.

**b.** Equality of access – there will be less chance of individuals feeling isolated as they are able to make use of social media, email, etc. People will also be able to interact with a wide variety of different people from different groups.

1. **a.** Some people may become socially isolated: for example, if they are housebound, they will not be able to order online.

**b.** Some people will not be able to access some services: for example, they will not be able to receive information from their council if the council only publishes it on their website.

1. **a.** More social isolation – people may be less likely to leave their houses to access information; for example, they may be less likely to visit libraries.

**b.** People may become more sedentary – for example, shopping from their couch rather than walking to a local supermarket. Society may become less healthy with increased obesity levels.

### Activity sheet 3.32: Is it legal?

#### Scenario 1

* 1. Age discrimination.
  2. Change the age categories – allow over 65s to enter.

#### Scenario 2

* 1. Equality.
  2. Agree to the purchase of assistive technology to enable the employee to carry out their   
     job role.

#### Scenario 3

* 1. Race relations.
  2. Make the advert neutral in terms of ethnicity – both groups should contain people of different ethnicities.

### Activity sheet 3.33: Is the net neutral?

#### Scenario 1

* 1. Yes – the ISP is favouring one streaming service over the other.
  2. Benefits: Faster download speeds for FastTunes users.   
     Drawbacks: Slower speeds for Lightning Media.

#### Scenario 2

* 1. No – this appears to be a decision by each company about its default streaming quality. This has nothing to do with the ISP.
  2. Benefits: Customers can choose the provider based on preferred sound quality.   
     Drawbacks: Customers may not realise this when joining FastTunes and so may be locked into a contract that gives them lower quality music than they would prefer.

#### Scenario 3

* 1. No – this appears to be a decision by the business about how to control bandwidth and offer two levels of service.
  2. Benefits: Customers can choose which level of service they want based on their needs and their ability to pay.   
     Drawbacks: Poorer customers may have no choice but to use the cheaper service and so are denied the chance to view websites based abroad.

### Activity sheet 3.34: Is it acceptable use?

#### Statement 1

* 1. Not acceptable. Employees could refer to customers in general and say anything derogatory, providing they don’t name them.
  2. ‘Employees must not discuss matters relating to their employment whilst using   
     social media.’

#### Statement 2

* 1. Not acceptable. Employees could cause damage or import malware and this would be acceptable under the policy.
  2. ‘Equipment provided by the employer, for example laptops and smartphones, must not be used by the employee for any private purpose.’

#### Statement 3

* 1. Not acceptable. Employees could refer to customers in general and say anything derogatory providing they don’t name them.
  2. ‘Employees must not discuss matters relating to their employment while using social media.’

#### Statement 4

* 1. Not acceptable. Instant dismissal is too severe a punishment.
  2. ‘Failure on the part of an employee to follow this policy will be met with disciplinary action which, in the first instance, may result in a verbal warning.’

1. **a.** Customers could cause physical damage and the business may not be able to take action.

**b.** Customers could cause damage to software and the business may not be able to take action.

1. **a.** Customers could cause physical damage and the business will be able to take action.

**b.** Customers will be more likely to understand what they can and can’t do when trying out the equipment.

1. Policy could refer to:

* need to respect equipment
* must not install software
* why certain websites are blacklisted
* consequences of deliberate misuse of the equipment or other non-adherence to the policy.

### Activity sheet 3.35: Does it comply with GDPR?

#### Scenario 1

1. Data must be adequate and relevant.
2. No – political party is not relevant.
3. Last item should be removed from the request and all such data deleted.

#### Scenario 2

1. Data captured for one purpose must not be used for another.
2. No – data can only be used for specified purposes – there is no right to be able to use data for any purpose.
3. The statement should be revised to reflect the above: that is, the reference to ‘for any other purpose’ should be removed.

#### Scenario 3

1. Data must be accurate and kept up to date.
2. No – if the error was the organisation’s own fault then, it should not penalise the customer for their own error. If it was the customer’s fault, then the business may not be obliged to send a free replacement but, in either case, the customer should not be charged to have this item of data edited for future orders.
3. The company should stop charging customers to have their personal data edited.

#### Scenario 4

1. Data must not be transferred to another country that does not have adequate data protection legislation.
2. No – the country where the consultant is based does not have adequate data protection legislation.
3. The company should not send this data to this consultant.

### Activity sheet 3.36: Who sees your digital footprint?

1. A small text file placed on a user’s computer by a website. They contain small pieces of data such as usernames and passwords.
2. First-party cookies are placed by the host website and enable it to provide its own services (such as remembering a username) better. Third-party cookies are placed by other organisations such as advertisers and enable the website to host third-party content   
   (for example adverts placed there by advertising agencies with the agreement of the   
   first party).
3. Third-party cookies enable an advertiser to remember the last advert shown by it on   
   Website 1; when you visit Website 2, the same advert can be shown.
4. You will no longer receive personalised ads but instead will see generic ads that may include products you do not wish to see (for example a vegan may see adverts for hamburgers).
5. Some users will not like this as it is an invasion of privacy. Others may be happy if it means that they can receive more personalised services.

### Activity sheet 3.37: How well do you understand intellectual property?

1. It means that the information has been copyrighted. This means that it is protected by law.
2. It means that the word or symbol is a registered trademark and so cannot be used by anyone else except to reference the trademarked product.
3. It means that the creator of the work has placed no restrictions on how it might be used.   
   You are free to copy or adapt it for any purpose.
4. You will need to obtain permission from the copyright holder to use the image. You will need to contact them and specify how you intend to use the copyrighted item. The copyright holder may place restrictions on how it can be used. They may charge a fee to allow you to use it.

### Activity sheet 3.38: Computer misuse at Trenshaw Media

1. The ‘website’ was almost certainly fake but looked like the real one – the journalist may have entered their security credentials, enabling the criminal to gain access to the bank account.
2. The file probably contained malware that, although not opening as a spreadsheet, might have attempted to install malware on the computer. This could have been key-logging software, which could enable a criminal to identify usernames and passwords.
3. The files may have included what the administrator thought were music files. They probably contained malware that was then was installed on the administrator’s computer, so gaining access to the network.
4. **a.** Unauthorised access:
5. Access rights for staff – limiting access to files needed for work purposes only.
6. Do not write down passwords.
7. Use two-factor authentication to log onto the network.

**b.** Unauthorised modification of materials:

1. Make files read-only for staff who do not need to edit them.
2. Amend staff access rights – some staff just have read-only access.
3. Ensure that back up systems allow any unauthorised modifications to be undone quickly by reverting to an earlier version.
   1. Spreading of malware:
4. Ensure that anti-virus software is up to date.
5. Limit staff ability to use external memory devices, for example USB sticks.
6. Use of virtual machines to separate different parts of the computer system from   
   each other.

# Activity sheet 3.39: Building skills for assessment activity

1. Doctors’ surgeries store highly sensitive data. The insurance company may have been able to access this data and therefore people may see this as an invasion of privacy.
2. If the insurance is targeted towards certain age groups, then the insurance company may not be able to correctly know the age of the patients.
3. The data will need to be changed into a universal format such as CSV which can then be exported and then imported into another device.
4. The surgery will need to comply with legislation such as data protection laws. For example, this law states that all personal data should be kept protected. Failure to protect data may result in a heavy fine.
5. **a.** Use the auto power-off setting on your computer to close and switch off if the computer has not been used for a period of time (maybe 30 minutes or 1 hour).
6. Use power saving settings on devices to reduce screen brightness, which saves power and means your device will last longer between charges.
7. **a.** Send data electronically such as email where possible.
8. Keep data electronic rather than printing documents.
9. **a. Send data electronically such as email where possible** – Keeping emails organised is more difficult than with traditional filing cabinets.
10. **Keep data electronic rather than printing documents** – This means that copies can easily be made and the data can be accessed in lots of locations, including by users who are not authorised.
11. **a.** Upgrade the computers such as changing the hard drive rather than simply replacing them.
12. Change the power settings so that they turn off when not in use.
13. Plagiarism is copying someone else’s work or intellectual property without acknowledging them, claiming it as your own.
14. • Ask the owner of the photo for permission to use it.

* Acknowledge the owner of the image when you use it.

1. The journalist would need to follow copyright laws by:

* Ask the owner of the photo for permission to use it.
* Acknowledge the owner of the image when you use it.

1. Cookies are text files that may be downloaded to your system without your knowledge while you are visiting a website. They contain information about the sites you have visited.
2. First-party cookies are stored by the website you visit. Third-party cookies allow users to be tracked across sites.
3. Cookies contain information about sites that you have visited. Therefore, if you have recently been searching for a particular product, this can be stored in your cookies. Websites can then search your cookies to see if any of their products may be ones that you are interested in, based on your history and personalise their adverts to you.

### Activity sheet 3.40: Information flow in a travel agency

1. To show how information is communicated (from source to destination; who sends and receives the information; can show one- or two-way communication).
2. How information flows around a system.
3. 6.
4. **a.** Stage 1. Holiday request: Customer makes a holiday request to the sales desk.

**b.** Stage 2. Accommodation request: Sales desk makes an accommodation request to   
the hotel.

**c.** Stage 3. Flights request: Sales desk makes a flight request to the airline.

**d.** Stage 4. Request for payment: Hotel makes payment request to the travel agent (billing).

**e.** Stage 5. Request for payment: Airline makes payment request to the travel agent (billing).

**f.** Stage 6. Request for payment: Travel agent (billing) makes payment request to the customer.

### Activity sheet 3.41: Data flow in a travel agency

1. To explain how data is processed by an existing system and how it could be processed by a future system.
2. **a.** Entity: a person, organisation or group that is interacting with the process.

**b.** Process: a series of actions or steps that do something to the data.

**c.** Manual data store: physical data store such as a diary or address book.

**d.** Digital data store: electronic data store.

1. **a.** 1.

**b.** 2.

**c.** 0.

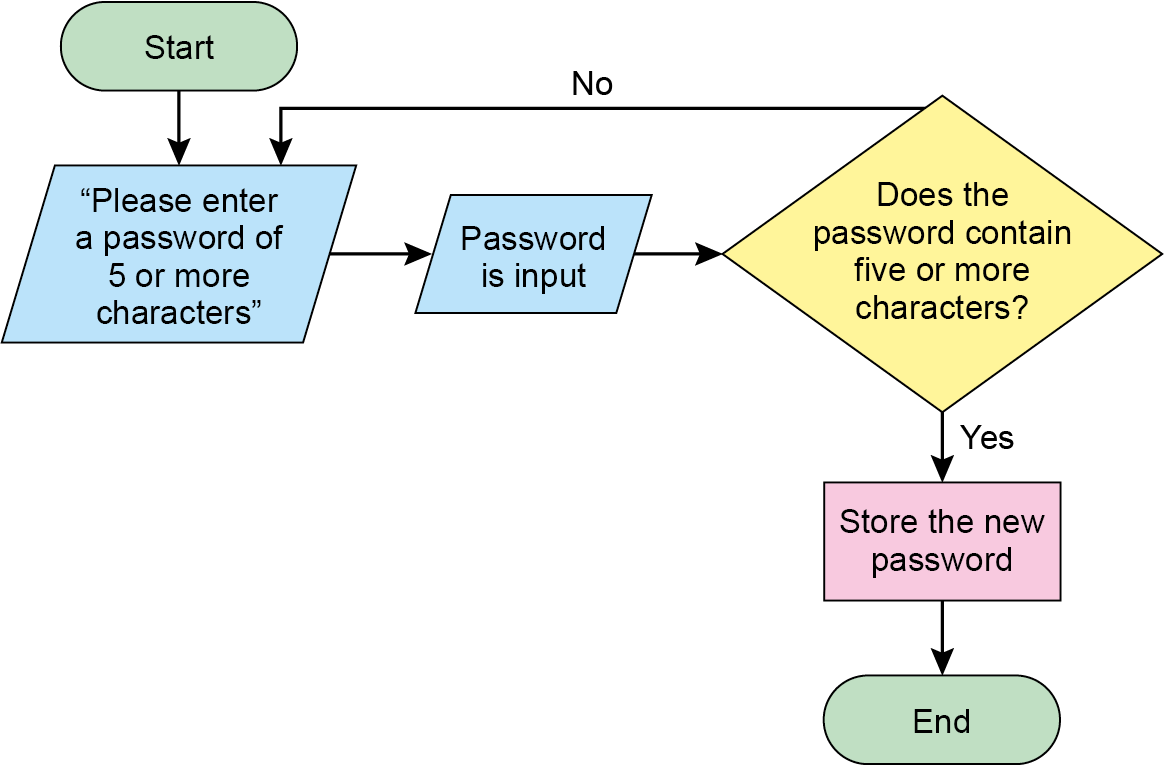
**d.** 1.

1. Customer makes accommodation request. Enquiries system makes a room availability request by looking up accommodation availability. If the accommodation is available this is passed back to the customer who places an order for the room. The booking system then updates room availability in the accommodation file and also requests payment from the customer.

### Activity sheet 3.42: Flow charts for a new online store

**1–4.** See page 210–211 of Student Book.

**5.**



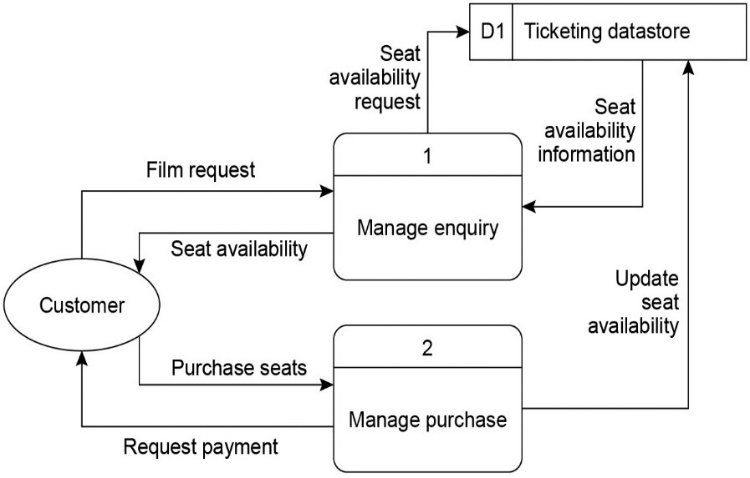
### Activity sheet 3.43: Interpreting system diagrams

1. **System diagram 1:** A customer communicates with an assistant in a travel agency – either face to face, by telephone or by email. The assistant contacts a hotel booking assistant by telephone to make the request. The hotel assistant checks availability in the hotel database and confirms availability to the travel agent. The agent passes this onto the customer who,   
   if the availability suits them, makes a booking via the agent – this is handled by the bookings database, which both updates the availability database and sends a confirmation email to the travel agent, who then passes this on to the customer.
2. **System diagram 2:** A seller posts details of a product for sale to an auction website using their desktop PC. A potential customer visits the auction website using their mobile device and makes a bid for the product. The auction website then contacts the buyer and seller to confirm that the bid was successful. The seller then posts the product to the buyer.
3. **System diagram 3:** A patient is unwell. They visit an online knowledge system and provide it with details of their symptoms. The knowledge system gives advice to the patient and also passes on the information to the patient’s doctor. The doctor then contacts the patient to discuss treatment.

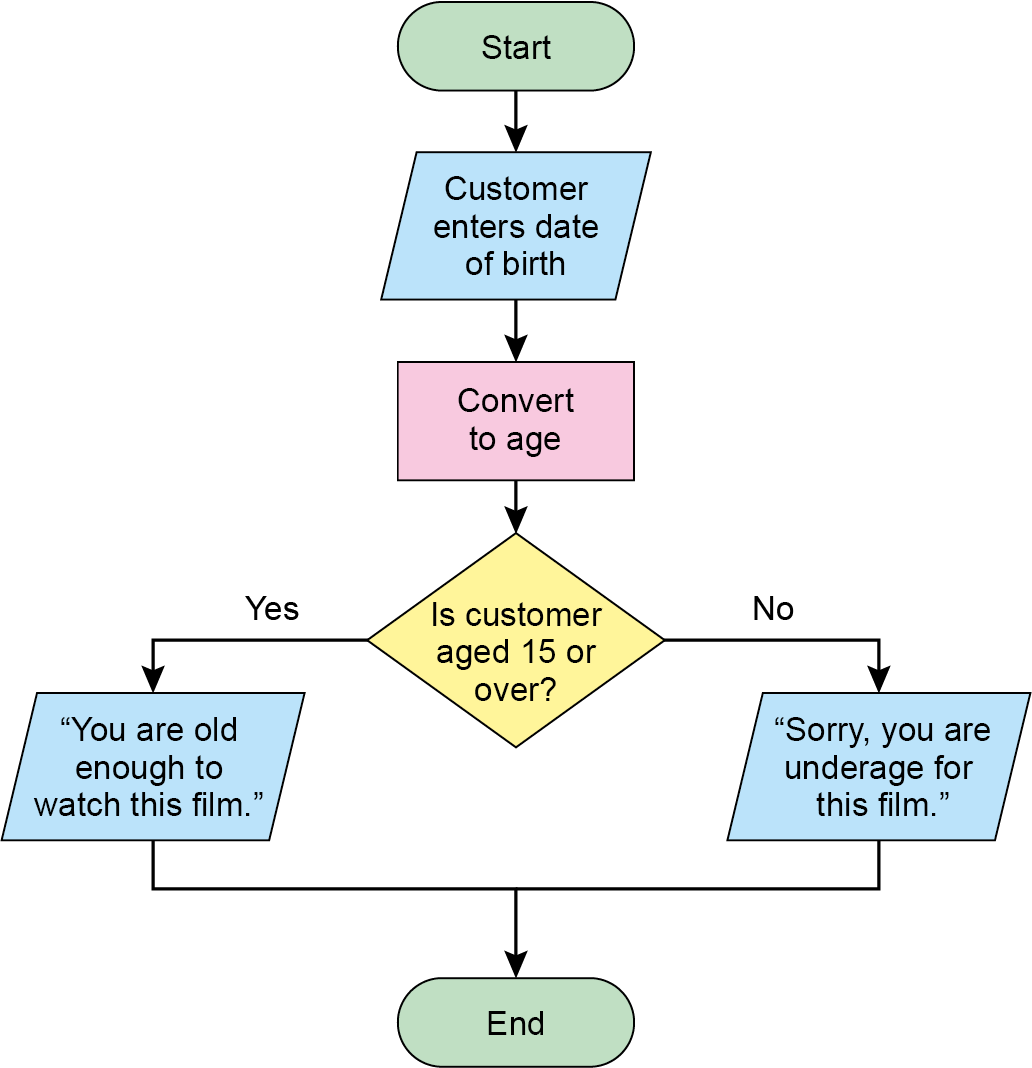
### Activity sheet 3.44: Using tables and written information

1. Word processor (906,000).
2. Database (144,000).
3. Word processor: absolute increase = 47,000, relative increase = 38%.
4. Yes, because a chart shows a visual summary of information; shows patterns/trends; enables key points of data to be understood quickly.   
   No, because a chart could present the data in a misleading way.
5. To describe the important points of a document.

### Activity sheet 3.45: Creating a data flow diagram for a cinema

****

### Activity sheet 3.46: Creating a flow chart for a cinema

****

# Activity sheet 3.47: Building skills for assessment activity

1. There are three processes. One process will accept the order. Another process will then check the stock levels to check if the order is in stock. The third process will then order new stock.
2. The supplier will need to be linked to another process that will check their own stock levels from a data source.

**3.**

Keyboards   
sold > = 20?

Start

Input number of keyboards

Discount = 20%

UK resident?

Enter country of residence

Delivery = Free

Delivery = Charged

End

Yes

No

No

Yes

1. **a.** Data flow diagrams demonstrate how data will be processed via a program. Database developers use data flow diagrams to explain how different data is connected and how   
    data is stored or processed.
   1. Flowcharts demonstrate how something works and the logic that is used to make decisions, and what happens when decisions have been made.
   2. System diagrams are used to show what hardware and software is used in a system.
   3. Tables can be used to organise data into columns to make it easier to read.
   4. Written information allows you to go into detail about something.