8.1 Individual, social, legal and cultural issues
Mark Scheme

Q1.

All marks AO1 (understanding)

One mark per challenge that is explained.

Information can be combined / processed / transferred in ways that were not previously possible; **A.** an example of this **NE.** there is a lot more data

Technology evolves quickly (so difficult for law to keep up with changes) // new types of crime become possible // some crimes are easier // future problems may not be understood;

Global nature of Internet means crimes may be committed in one country from outside its direct jurisdiction // laws are often national/local whilst the Internet is global // digital crime can be committed from a great distance // different countries have different laws;

Some crimes may be committed by states rather than individuals;

Different countries / cultures may have different attitudes to principles important to computer science (such as copyright, intellectual property, privacy); **Note:** this point relates to attitudes not legislation

Methods such as encryption make it harder to monitor criminal activity // electronic evidence may be harder to gather than physical evidence // can be harder to identify culprits online (eg by use of proxies, VPN) // peer-to-peer systems make it harder to identify criminal; **NE.** hard to catch criminals

Individuals may have access to large amounts of sensitive information that may be of public interest // conflicts between freedom of speech/information and privacy / state secrets;

Technology companies (can use their wealth) to lobby for their own interests // concern over influence of companies on legislators;

Resources required to enforce legislation may not be available;

NE. Copyright, Data Protection, Misuse, Hacking

Refer responses containing other relevant points to team leaders.

Max 3

[3]

Q2.

Marks are for AO2 (analyse)

Level of response question

Level	Description	Mark Range

3	A line of reasoning has been followed to produce a coherent, relevant, substantiated and logically structured response. The response covers ethical, legal and cultural issues. In these areas, there is sufficient detail to show that the student has a thorough level of understanding of the issues involved. Although understanding would be indicated by two or three points being made in each of the areas, potentially thorough coverage of two areas might exceptionally lead to a mark in this band.	7-9
2	A line of reasoning has been followed to produce a mostly coherent, relevant, substantiated and logically structured response that covers at least two of ethical, legal and cultural issues. In at least one of these areas, at least two valid points must have been made that demonstrates a good understanding, and typically students should have made at least two points in two areas.	4-6
1	A few relevant points have been made and there is limited evidence that a line of reasoning has been followed.	1-3

Points may include:

Ethical:
Consider if material in images could be of harm to children.
Identifying and requesting permission from any members of public caught on the images.
Members of the public may not be as happy being photographed in a building as they are on the streets.
Recording of adverts could lead to unfair product placement.
Considering what harmful uses users of the system might use the captured images for.
Considering how often Google should update the image data.
Dealing with copyrighted information that might have been inadvertently captured.
Considering that access via Street View might reduce the number of paying customers for museums.
Are young people being dissuaded from leaving home to visit public buildings leading to poor health.
Need to consider which areas of a building are appropriate to film (eg toilets, offices, research laboratories)

Legal:
Does Google need permission to film in what might be a private building.
It may not be legal to film people without permission (on private land).
Aspects of data protection legislation might apply.
Copyrighted information might be inadvertently captured and may lead to legislation breach.
Consider if material in images is legally allowed to be viewed by children.
Could be a risk of identifying items to steal leading to liability for crimes being carried out.
Ability to identify locations and access could be used for crime or to carry out acts of terrorism.
Street View is a worldwide service so would need to consider different legal

systems.
Consideration of the security of information storage needs to be made.
Laws for certain buildings or areas of buildings may be more restrictive than others.

Cultural:
Some images of people or exhibits may be offensive to certain cultures.
Taking images inside religious buildings for some purposes may be considered inappropriate.
Some cultural beliefs may not allow photography of people.
Do people have the right to request the deletion of their images?
Could the culture of visiting places such as museums (e.g. family/school day trips) be affected by access to them online?
Need for balance between cultural sensitivities and freedom of expression.

NE. Without suitable context: Faces need to be blurred out, must comply with laws, invasion of privacy.

R. Reference to private homes, implication that will be used for live monitoring.

[9]

Q3.

Marks is for AO2 (understanding)

Level	Description	Mark Range
4	A line of reasoning has been followed to produce a coherent, relevant, substantiated and logically structured response. The response covers all four areas indicated in the guidance below and in at least three of these areas there is sufficient detail to show that the student has an excellent level of understanding of the issues and technologies involved. To reach the top of this mark range, an excellent level of understanding must be shown of all four areas.	10-12
3	A line of reasoning has been followed to produce a coherent, relevant, substantiated and logically structured response but the response may only cover two or three of the areas indicated in the guidance below. A good understanding is shown of each of these areas and if only two areas are covered, the coverage of these is excellent.	7-9
2	A limited attempt has been made to follow a line of reasoning by covering at least two of the topic areas in the guidance below. Overall, at least four valid points must have been made which can relate to any of the topic areas in the guidance.	4-6
1	A few relevant points have been made but there is no evidence that a line of reasoning has been followed. The points may only relate to one or two of the four areas from the guidance or may	1-3

	be made in a superficial way with little substantiation.	

Guidance – Indicative Response

1. How it was possible for data to be collected

WiFi signals can travel outside of property // over wide area // limited control over range

Any WiFi receiver in range can read the data packets **NE**. The receiver in the car can read the packets

No need to physically "tap" into a WiFi connection, unlike a cabled connection

A protocol that does not encrypt the transmissions may have been used // unencrypted data sent. **NE**. Network not secure

2. Steps to prevent

Use a protocol that encrypts data transmissions

A. Encrypt the transmission

R. Password protection

Example of secure protocol eg WPA, WPA2

Disable broadcast of SSID to make network harder to identify (Note: Accept this point even though the SSID would be in other data packets)

Limit power of transmitter so data does not travel outside premises (although in practice this might be hard to achieve)

Use cabled network instead of WiFi.

R. MAC address filtering (as cars were not connecting to networks just intercepting transmissions)

3. Legal and ethical issues

If the data is being transmitted through the air, who does it belong to, if anyone? // Should data transmitted by WiFi be treated like a broadcast (eg TV) or a private communication (eg telephone call)?

Is it wrong to intercept data if people freely choose to transmit it wirelessly? **A**. Is it ethical to collect data from people without their permission?

Is it legal to intercept data if people freely choose to transmit it wirelessly? What laws apply in this scenario? Is this really hacking?

Are the ethics or laws different for intercepting data transmitted wirelessly than by cable?

Is there a difference between collecting statistical data eg channel number, signal strength, SSID and collecting the payload data?

Was the data just collected or was there an intention to process it as well?

What should the company have done when it realised that the data had been collected? // Should the data have been immediately deleted, or kept so that the company could contact and apologise to people it had collected data from? // What should be done with the data now?

What should the company have done if it inadvertently discovered evidence of illegal activity in the collected data?

Legality/ethicality may depend on the nature of the data gathered // (In the UK) would some of the collected data count as "personal data" (under the Data Protection Act) // could some of the data have been sensitive (accept example eg

bank account details, details of minors) **NE**. Data may be private

To what extent is the company financially liable for collecting the data? Or any consequences of its use?

Could the legal situation be different in different countries where the company operated?

Was the collection of data intentional or just an accidental side-effect of a reasonable process?

What was done to ensure (existing) policies are followed?

Should there have been more oversight of code development?

Could intellectual property have been inadvertently stolen?

Is it ethical to collect/store information secretly from people // without them knowing?

Is it ethical to collect data if there is no (legitimate) purpose for doing so?

Were the developers in breach of their contracts with the company / company guidelines?

Relevant Legislation

Students may name specific pieces of legislation that could have been breached as part of their response. Determining whether or not a breach has actually occurred would probably require more information than is provided in the question and detailed knowledge of the legislation, which is not required by the specification. Therefore, up to **two points** can be given for students naming relevant pieces of legislation that could have been breached, regardless of whether or not this can be ascertained with certainty. Relevant pieces of legislation include:

- The Data Protection Act
- The Computer Misuse Act
- The Regulation of Investigatory Powers Act
- The Communications Act

Points should be given for assertions that legislation has definitely been breached, even if this is only a possibility in the context rather than a certainty.

Responses that reference other legislation should be referred to Team Leaders.

A. As an alternative to naming the Data Protection Act, a response could instead question whether privacy laws have been breached, or if a breach of privacy has occurred.

4. Lessons

Improved training for developers in what is legal / ethical (accept company needs to improve understanding of legal/ethical issues)

Need to review guidelines that developers are expected to follow

Need for scrutiny of code / supervision by people outside of development team

Developers could be required to check each other's code

Developers could be required to log changes made to code and reason

Should only collect data that is absolutely necessary // that has a clear purpose // need to review collected data to see why it is being collected and stored // need to fully consider the purpose of any data collection before doing it

Could/should remove equipment for Wi-Fi data capture used in cars to collect mapping data.

NE. Further testing should be carried out unless there is a clear explanation of the mechanism by which testing will check that the software has no additional functionality is described eg inspection of collected data files to verify purpose of

contents

[12]

Q4.

(a) 1. a mechanical / moveable structure;
2. can sense its surroundings / environment;
3. can manipulate things// interact with things;
4. makes dextrous coordinated movements;
5. has some degree of intelligence or ability to make choices based on environment;
6. is programmable // controlled by a computer system;
7. a mechanism guided by automatic controls // autonomous operation;
8. a machine that replaces a human being and performs various tasks of a human being // can operate in places / situations humans can not;
9. a device that automatically performs complicated / repetitive tasks;
10. a mechanism which reacts to its environment;
11. capable of consistent application / precise movements;
12. Should obey Asimov's laws // A robot may not injure a human being // allow a human being to come to harm;

MAX 2

(b)

Marking	
0 marks	student makes no valid points
1 mark	student makes a valid point
2 marks	student makes two or more valid points but these are not developed or connected
3 marks	student makes at least two or more valid points that are connected and leads to a final opinion

The following is a collection of examples that students could use to support their opinion.

YES:
Programs have been developed to mimic 'intelligent' behaviours such as playing chess;
Technology is moving on at a very fast pace;
AI research has shown that computers can 'learn';
Research into how the brain works is continuing to reveal new insights;
Evolutionary algorithms // adaptive algorithms // computer can modify their own programs;
Computers are getting closer to passing the Turing test (which is a test for intelligence)

NO:
Computers cannot learn to the same extent as humans and therefore cannot demonstrate intelligence;
Computers lack emotion / feelings / instinct / creativity;

Computers find it hard to cope with unexpected situations / work well only in a structured environment;
Hard to actually state / define what intelligence is;
No computer has passed the Turing test (even though this has been around for a long time) // due to the Chinese room / box argument;
Theological / existential reasons // intelligence can only be bestowed by a God;

Note: marks can be awarded for other valid statements - refer to team leader for discussion

MAX 3

(c) (i) a person who breaks through some security systems to gain access to a computer system;

1

(ii) Computer Misuse (Act);

I year

1

(iii) a global crime as criminals can easily be in another country;
use of botnets means that computers used are separate from and do not belong to the criminal // hacking might be routed through multiple computers // use of public computers / wifi;
use of IP spoofing //changing / dynamic IP address // use of proxy / vpn;
companies rarely wish to report that they have been hacked // bad publicity;
often difficult to detect that a crime has been committed // no physical / biological evidence;

Any other good reason - refer to team leader if in doubt.

MAX 2

[9]

Q5.

(a) **1** ;
4 ;
3 ;

3

(b) (i) Optical Character Recognition;

1

(ii) Data that can (uniquely) identify a living person;

1

(iii) *Linked to context*: **(MAX 2)**
Data could be used to track location (and activities) of a person;
Data links a person to a specific location and car at a (specific) time;
Number plates might not be recognised accurately (suggesting, incorrectly, a car was at a particular location);

General points: **(MAX 1)**

Concern over security of data storage / / security of data might be at risk;
Selling on of data;
Data used for marketing / / unwanted phone calls;

MAX 2

[7]

Q6.

(a) Data Protection (Act);

1

(b) Data should be kept securely;

1

(c) Data should be fairly and lawfully processed;
Data should be obtained for specified and lawful purposes. (**A** Data should be processed for limited purposes);
Data should be adequate, relevant and not excessive;
Data should be accurate // kept up to date;
Data should not be kept longer than necessary;
Data should be not transferred to other countries without adequate protection;
Data should be processed in accordance with the rights of the data subjects.

Max 1

(d) That data is not being encrypted // data is not being sent securely // that hackers might be able to see personal data;
A the protocol / it is not secure
R website not secure

HTTPS // HyperText Transfer Protocol Secure;

2

(e) Word processor : General purpose (application software);
Parent portal : Bespoke;
Web server : Special purpose (application software);

3

[8]

Q7.

(a) Copyright, Designs and Patents (Act);
A Digital Economy Act

1

(b) No money goes to the artists / publishers / distributors;
The quantity/amount of music being produced could go down;
(Pirated) music can be of a lower quality;

Max 2

(c) Can sell on items that have been purchased;
Can play on any suitable device // Can be played on many devices that the purchaser might own;
Can make backup copies;
Can play without any time limit// no limit on amount of plays;
Can load into any suitable software package;
Encourages creativity / sharing / remixing / reworking;
A user has full control over their music

Max 2

[5]

Q8.

(a) (i) To manage / control / execute commands on a remote machine;
A remote access / login
A a clear example of remote management
NE remote viewing
R remote desktop

1

(ii) Enable files on one host / computer / client to be copied to another host / computer / server;
To manage files on a remote computer / server;
A to upload / download / transfer files
NE "sharing"
NE load a file
NE transfer data

1

(iii) To retrieve / fetch (stored) email;
To check for <u>new</u> emails;
A access / download / receive
R sending
TO any mention of sending
NE just "email"

1

(b) (i) 192.168.3.205 // 74.125.4.148 // 208.43.202.29;

1

(ii) 80 // 25 // 58539 // 57458 // 57459;
I colons

1

(iii) 192.168.3.205:80 //
192.168.3.205:25 //74.125.4.148:58539 //
208.43.202.29:57458 // 208.43.202.29:57459 ;

1

(c) Servers might be in another room / site / cupboard / inaccessible ;
Servers might not have a keyboard / monitor installed ;
Can manage multiple servers from one machine;
Servers can be managed outside of work hours / from anywhere;
It would be quicker (**A** more convenient) (to manage from her machine than visit the servers) // better time management;
Server rooms are often uncomfortable places for people to work in;
NE she does not need to go to the servers

Max 2

[8]

Q9.

(a) **Legislation**
Health and Safety (Regulations);
Display Screen Equipment Regulations;

Affect
Monitors should be moveable / adjustable to alter height / reduce glare / minimize flicker;
A top of screen at eye level
Chairs should be moveable / adjustable;

Position of mouse/keyboard assessed // keyboard should be separate from screen;
Consideration of lighting;
Space under desk for legs;
Supply a foot-rest / wrist-supports;
A feet should be touching flat surface
Set up software to use readable fonts // select colours that are easy on the eye;
Cables should not be left loose;
Sufficient workspace around computer;

Max 1 mark for legislation
Max 2 for affect

3

(b) (i) Copyright, Designs and Patents (Act) ;
R Copyright

1

(ii) Number of licenses the library has;
If the software needs a license;
Type of license the library has;
Library has a site-wide license;
Check that software can (legally) be used on more than one machine;
A its terms of use

Max 1

(c) Contract/rules/regulations that an employee must follow // a member of an organisation is bound by;
NE agreement/terms
R Laws alone instead of rules
Contents of a code (may) not be legal requirement;
Breaking rules could result in disciplinary action/possibility of losing job;

Max 1

[6]

Q10.

(a)

Purpose
To distribute commercial software
To store a 20GB high definition movie file
To use for a 3GB archive of a school server
To create a copy of a music album

Note: Mark first occurrence of each medium

4

(b) **Write**:
To write data a high powered / high frequency laser makes sections less reflective / burns a pit;
R laser writes grooves/tracks;

Read:
A low powered laser is used to read data back from the disk;

Mechanism:
The difference between reflective and non-reflective parts / pits and lands indicates the 1s and 0s;
The data is stored as a continuous spiral track;

One mark each for write, read and mechanism.
Note: a laser is used to read and write data (1 mark only)

Max 3

(c) No hardware exists to read CD-R disks;
The CD-R medium has become corrupted // CD-R is scratched / damaged / degraded;
Support for file format no longer available // no software capable of reading format data stored in CD-R;

Max 2

[9]

Q11.

(a) An ISP sells clients Internet access/connection; Provides users with access to Internet backbone;
R provides an Internet service

Max 1

(b) Clients may have broken Copyright, Designs and Patents Act;
Digital Economy Act;
R Copyright, Copyright Act

Max 1

(c) Data which relate to a living individual who can be identified from that data // data about a living identifiable person;

1

(d) (i) ISP has (potentially) broken Data Protection Act (by not securing personal data);

1

(ii) (Clients have potentially misused / hacked their ISP's computer system) therefore clients have broken the Computer Misuse Act;
R they may have broken the law

1

[5]

Q12.

Exactly same operation performed over and over again by programmed robot sprayer;
Position of car bodies predetermined//car bodies in known precise positions all the time//
Robot sprayer does not need to deviate from pre-programmed position at any time // a strictly controlled environment;
Actions to be performed known in advance for programmed robot sprayer;
Programmed robot sprayer requires only limited sensing of environment if any // fewer inputs to monitor;
Robot sprayer does limited processing;
Robot sprayer has a relatively simple program which is numerically controlled;

Car system has to continuously monitor many external variables;

Car system has to perform very complex processing;
Car system will need very powerful processors;
Car system will need a range of sensors;
Car system has to analyse/react to an input very quickly (and then adjust one or more of the three given outputs to alter car motion);
The environment in which the car operates is not predictable//is more complex//has greater uncertainty;
Car system needs to know at all times exactly where it is;

Candidate may answer by example, e.g.
Car system cannot be programmed in advance to know where all pedestrians will be at any one time //
Car cannot be programmed in advance to know where all other moving cars will be at any one time //
Car system cannot be programmed in advance to know where all stationary obstacles such as parked cars will be//potholes at any one time;

Note: For full marks candidate must cover both problems

Max 4

[4]

Q13.

(a) Copyright Design and Patents Act (1988) // Copyright and Related Regulations (2003) // Digital Economy Act (2010);
NE Copyright, Copyright Act

1

(a) Encrypt the music file;
A (decrypt) key is needed for playback; **R** code, PIN, password for key
Download server keeps records of authorised clients (hardware devices) allowed to decrypt music; R tied to IP address
Playback tied to a particular (set of) hardware device(s);
A Using a digital watermark in the music file a form of steganography;
R cannot be transferred to other devices
NE "player" for "device"

Max 2

[3]

Q14.

Good at:
Can make precise/accurate / complex calculations / actions;
NE "good at maths / logic" – need the concept of complex
More consistent than humans;
Repetitive tasks;
Can work in conditions too dangerous for a human;
Working with large volumes of data;
Fast processing of data / calculations;
Can perform task without breaks / / for longer than humans;
R don't get bored

Bad at:
Image recognition;
Shape detection;
If the conditions change they adapt poorly / / not very adaptable / / learning;

A “can’t think for themselves”
Poor at coping with emergencies / unexpected circumstances;
Creativity / / invention / / lateral thinking;
Bad at discriminating;
Processing qualitative data;
Recognising human concepts e.g. emotion;
A Cannot recognise when it makes mistakes;

Above are exemplars only. Award credit for other valid points.
Max 3 if all points are about just good or just bad.

[4]

Q15.

(a) Name or description of any task that is likely to be completed by a robot;

1

(b) Task is repetitive / monotonous;
Precise movement required;
A accurate movement
Consistent task completion;
Robot gives increased productivity / faster than human;
Task is unpleasant;
Task is dangerous/improved safety/reduced risk to humans;
Robot able to operate in environment human could not work in;
Continuous operation;
R humans get tired / need a break
Cost effective in the long term;
R cheaper, “no wages”
Response must be valid within context of task named in part (a)

Max 2

[3]

Q16.

Arguments for DRM:
Protects *copyright* // makes it harder to breach copyright/pirate works / restricts sharing the music;
Ensures creators/suppliers receive payment for work;
Preserves incentive for people to develop new works / promotes continuation of business;
Facilitates online rental service;

Arguments against DRM:
Restricts the potential audience;
Content difficult to access as encrypted;
Makes it difficult for purchasers to make legitimate copies / backups;
Prevents use on multiple devices // tied to one or a small number of (hardware) devices;
Ineffective at preventing copying / example of why ineffective;
Can restrict playback of music to particular software packages / competing systems incompatible;
May be unable to listen to music if company ceases to exist / relies on company continuing to exist / unable to listen if can not authenticate copy // unable to listen if NO Internet connection;
Does not deal with expiry of copyright period;
Limits creativity / limits collaboration in creating content;

To achieve a mark in this band, candidates must meet the subject criterion (SUB)

and 4 of the 5 quality of language criteria (QLx).

SUB Candidate has provided a balanced argument for and against DRM (**at least two points on either side**) , making at least 5 distinct points.

QL1 Text is legible
QL2 There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear.
QL3 The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently.
QL4 Sentences and paragraphs follow on from one another clearly and coherently.
QL5 Appropriate specialist vocabulary has been used.

5–6

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

SUB Candidate has made at least three points. Additionally, to get four marks, **there must be at least one point on each side** of the argument.
QL1 Text is legible
QL2 There may be occasional errors of spelling, punctuation and grammar. Meaning is clear.
QL3 The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.
QL4 The candidate has used well-linked sentences and paragraphs.
QL5 Appropriate specialist vocabulary has been used.

3–4

To achieve a mark in this band, candidates must meet the subject criterion (SUB). The quality of language should be typified by the QLx statements.

SUB Candidate has made one or two relevant points.
The answer may be one-sided.
QL1 Most of the text is legible.
QL2 There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response.
QL3 The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.
QL4 Sentences and paragraphs may not always be well-connected or bullet points may have been used.
QL5 Specialist vocabulary has been used inappropriately or not at all.

1–2

Candidate has not made reference to any of the points listed above.

0

Note: Even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question.

If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 3 of the quality of language criteria are met in the lower band. If 3 criteria re not met then drop by two bands.

[6]

Q17.

(a) (i) Copyright, Designs and Patents **A** Copyright

1

(ii) Computer Misuse

1

(iii) Health and Safety at Work **A** Health and Safety

1

(b) (i) Rules that an employee must follow//a member of an organisation is bound by;
NE agreement
R Laws alone instead of rules
Usually a (written) document/contract;
Contents of a code (may) not be legal requirement;
Breaking rules could result in disciplinary action/possibility of losing job;

Max 2

(ii) To set out points of good practice for employees//set out rules that are not legal requirements;
To ensure employees are aware of legal requirements//as employees may not know what the law is;
To relate legal requirements to the work that the employee does;
To make clear consequences of breaking the rules *if mark not already awarded in b(i)*
A to exonerate the company if law is broken

Max 2

[7]

Q18.

(a) Data that relate to a living person // individual who can be identified from that data;
NE Data that belongs to / relates to a person

1

(b)(c)

Principle	**Appropriate Feature**
Data must be accurate and up to date. **A** accurate without up to date or vice-versa (**A** correct for accurate)	Validation / examples of a validation method; Verification / example of a verification method; Store date when data last updated; Alert user when data is older than specified age;
Data must not be kept for longer than is necessary.	Password / card / biometric to logon; Encryption; Backup; Different types of user / users have different rights; Automatic logoff if left unattended; Other appropriate security

	method;
Data must be processed in line with the rights of data subjects.	Option to flag customer as not accepting direct marketing; Option to edit or delete data; Option to print copy of all data for customer to see;
Data must be kept securely // Prevent unauthorised access / disclosure of data **NE** Hacking	Records deleted automatically after no contact with customer for fixed period; Option to delete data;
Data must only be processed for registered / lawful purpose	Input of data subject preference with regard to use of/transfer of data; Restrictions on exporting data from package;
A Data must not be transferred to other countries without adequate protection.	Restrictions on exporting data from package;

*1 mark for **principle***
*1 mark for **naming feature** that is appropriate to the principle stated*
*1 mark for appropriate **explanation of how** the feature will help the company comply with the DPA*
R Other DPA principles
Mark can be awarded for principle if no feature stated or if feature inappropriate.

3

[4]

Q19.

(a) **What**:
Access management system for digital media;
Method of encrypting digital media;
Media can only be read/used/accessed with correct key;

Why:
To enforce copyright law // Protect intellectual property;
A Prevent criminal offence
R Just illegal
To stop people copying music (without permission)/prevent piracy/prevent illegal sharing/prevent illegal downloads;
R stop reselling
To ensure company/artist receives income from sales of music // does not lose money;

Max 2 for what, max 2 for why, max 3 overall

3

(b) Music/files are encrypted;
R Encoded/Scrambled for encrypted
User obtains key when purchases track/file;

Music/files must be decrypted with key;
R Password, Code
Key may only work on computer file downloaded onto;
A Playback tied to particular hardware device/group of devices
R Files cannot be copied
Key may need to be authenticated with server over Internet whenever file used // Company may have licence/key server;
Time lock so music will not play after certain date // only play a fixed number of times;
Use of a specific/proprietary program to play music;
Usage rights may be expressed in a Rights Expression Language;
R Streaming;

Max 2

[5]

Q20.

(a)
1. a mechanical, moveable structure;
2. can sense its surroundings/environment;
3. can manipulate things;
4. // interact with things;
5. makes dextrous coordinated movements;
6. has some degree of intelligence or ability to make choices based on environment;
7. is programmable;
8. a mechanism guided by automatic controls;
9. a machine that resembles a human being and performs various complex tasks of a human being;
10. a device that automatically performs complicated/repetitive tasks;
11. a mechanism which moves and reacts to its environment;
12. a robot is a mechanical or virtual Agent;
13. artificially created;

Max 2

(b) **Application:** *(or any other reasonable for 1 mark)*
manufacture / welding / bomb disposal;
Why: *(max 1 mark)*
1. repetitive tasks;
2. tasks that require precision;
3. tasks that are dangerous for humans;
4. produces consistent quality
5. continuous operation;

2

[4]

Q21.

(a) (i) **Unauthorised access**
Password protect sensitive files;
//have username & passwords to log on;
/ have username & password / use biometrics to restrict access;

1 mark

AND
Change passwords on a regular basis;
/ choose passwords that are difficult to guess;

/ do not write passwords down;
/ shut down after (e.g.) 3 attempts at guessing the password;
***A** and set attributes/permissions/access rights;*

1 mark

//Set attributes/permissions/access rights;

1 mark

AND
To restrict access to specific users or groups of user;

1 mark

//Use biometrics /lock doors to rooms where terminals are
/employees log off / lock machines when they leave them;

1 mark

AND
To restrict access to sensitive files to certain terminals;

1 mark

// encrypt (sensitive) files;

1 mark

AND
Only authorised users have (decryption) code/key;

1 mark

(ii) Use software that can monitor /log user activity
A record
R store /monitor file changes;

1 mark

4

(b) (i) **Data protection**
Firewall;
A 'strong' passwords
A Encrypt data ;

1

(ii) Use up to date virus checking software;
A Regular backups (*if not given in iii*)

1

(iii) Regular / automated backups;
/Uninterruptible power supply; (so that system can be shut down safely)

1

(c) **Restore**
A good recovery / restore procedure;
A description of this
/backup media must be available immediately;

/ availability of alternative hardware;
A Make regular backups *if not given in (iii)*
A have a contract with an outside recovery service;

1

[13]

Q22.

Device	use	why
RF Remote Control	User can switch appliances/lights on (and off from a distance) // open/close doors/curtains;	does not have to be in line of view; (as with an infra-red device)
Movement Detector	Lights could switch on as user is approaching a new area // Doors could open on approach;	would be difficult for a wheelchair bound person to reach the doors/lightswitch;
Voice recognition system	To open/close doors/curtains // activate lights;	User could speak commands rather than pressing buttons // Don't have to reach button;
CCTV	See who is outside/rang the doorbell;	Without going to the door;
Fingerprint door locks	To control who gets through the front door // to lock/unlock front door;	without needing a key;
Climate control system	to get fresh air // control temperature in house automatically;	No need to open windows // no need to adjust air con/heating manually;
Motors to operate doors/curtain rails	Can control opening/closing of garage door/door/curtains;	would be difficult for a wheelchair bound person to reach the doors/curtains; without the use of manpower; **A** for client to move around more easily;
Switching Unit	To switch on motors for curtain rail when it gets dark/ at certain times of day // to program the switching on of lights/heating/multimedia system/ according to times of day/week ;	Automates daily/regular activities so less to do manually;

C/F or C/B between 'Use' and 'Why'
Note: 'would be difficult for a wheelchair bound person' on its own NE. Needs context of use.

2 marks max for each explanation

[6]

Q23.

(a) **Social;**
Some people get so many junk e-mails/ spam take up so much space;
That they have to change their e-mail address;

That legitimate e-mails get submerged by them;
Service degrades;
//Some ISP's spam filters;
Reject legitimate e-mails;
// unkind / spiteful/ gossip type e-mails;
Can be spread about a work colleague / ex 'partner';

Max 2

Economic
Wastes resources;
Dealing with junk e-mail;
// corruption /damage to software and data;
From viruses carried by spam;
//many spam are fraudulent;
People pay for things that never arrive;
// ISPs have to pass on the cost of extra bandwidth;
To their customers; (Spam slows down Internet)
//people with dial-up connections
/ who receive e-mails on mobile phones;
Have to pay to download the junk mail;
Cost of;
Spam filters;

Max 2

Ethical;
People / vulnerable adults upset by;
Obscene / inappropriate e-mails;
Phishing e-mails;
Extracting personal /financial information;

Max 2

A ethical - social, economic - social cross over where valid, but points must be different.

6

(b) Have more than one e-mail address;
Use a spam black-list to refuse e-mails from known spamming sites;
Use a spam filter in the e-mail software / in house;
Careful choice of e-mail address;

1

[7]

Q24.

(a) **Copyright (not license) is**
The (economic) right of the writer / vendor of software to control the use / availability of their material;

1

(b) **A purchaser can legally:**
Install / Run the program on a computer;
// Run the program on the number of computers specified in the license;
A Make a single copy for back-up purposes
A Use it for personal use

1

(c) **A purchaser cannot:**
Make a copy (to give to a friend);
Run it on more computers at once than you have a license for;
(accepted as different from above if specified clearly)
Copy and sell the software;
Convert the program into another computer language;
Transmit it (over a telecommunications line);
Reverse engineer it;
R rent it, lend it

1 mark per point to a maximum 2

2

[4]

Q25.

(a) *1 mark for one **benefit** to each of (i), (ii), (iii) to max:*

(i) **UK Universities:**
Economic – can charge realistic (i.e. more than for British students) fees to overseas students;
Economic – generate more revenue by enrolling more students;
Economic – they feel they need to as their competitors are /it threatens their client base;
Economic – ease with which material can be updated;
Economic – can expand without providing more buildings / reduced staffing because on - line;
R fewer lecturers
Economic / Social – world-wide publicity / respect;
Social – seen to be inclusive of e.g. people who cannot study full time;

(ii) **Students:**
Social – different time zones no problem œ can study at any time of day;
Social – can continue the course even if they don't stay in one place long enough;
Economic – no travel or accommodation expenses / can live at home;
Economic – can fit study round other commitments such as work;

(iii) **Businesses**:
Economic – can attract and keep the best staff with the promise of further good qualifications;
Economic œ More effective / skilled / knowledgeable / motivated workforce possible;
Economic – employees can apply their learning to their work immediately;
Economic – training of employees can be done at times convenient to the business;

3

(b) **Hardware*:***
Modem / cable modem ;
ISDN line / ADSL Line ;

1 mark

Software:
Browser;

Communication software / dial-up software;
Online teaching software;
Discussion forum / bulletin board software;
Telnet / ftp software / remote access software;
***R** IE / Netscape etc.*

1 mark

2

[5]

Q26.

(a) (i) People listening to audio CD often want to know the title of the track without having to look this up on CD cover;
Additional information not recorded on CD cover may be available from on-line database;
User can get e-mails promoting products that user likes;
User may get sent information related to interests;
Filtered information can be sent to user based on user's interests;

1

(ii) Could gain statistics based on user interests;
Could expand product line to cater for users' interests (generating more revenue);
Could mean lower marketing costs for company because marketing is targeted;
Could mean cheaper audio CDs because company spends less on marketing (leading to more sales);
Could mean discounts on audio CDs for listener leading to more sales);
Marketing information can be sold on;
A Targeting related to costs/revenue answers
R could sell more CDs unless justified with a response that maps onto above
R Marketing can be targeted **R** Can detect piracy **R** Costs alone

1

(b) Invasion of privacy//user isn't aware of this taking place;
Computer owner's permission to link e-mail address to digital fingerprint not obtained;
Permission to place digital fingerprint on user's computer not obtained;
Because users may not want their tastes in music to be known;

1

[3]

Q27.

LAN;
Justification:
Computers in health centre are in close proximity to each other/geographically close/in same building/on same site;
R Computers within health centre on its own

[2]

Q28.

(a) International transfers span different time zones;
Messages may get lost otherwise;

Transfers may be batched for transfer overnight;

Max 1

(b) To prevent fraud;
To prevent changes to the message going undetected;
To prevent changes to the content of the message;
To prevent message being understood or information gathered;
R To prevent a message being read…….

Max 1

(c) N.B.Emphasis is on government monitoring banking transfers for something illegal
To make it possible for agents of the government to learn of money transfers made by criminals;
To make it possible for agents of the government to learn of money transfers made by terrorists;
R So government can monitor messages/e-mails.

Max 1

[3]

Q29.

(a) *Any two reasons × 1 each*
To monitor criminal activity; (accept two different types of each category)
(**A** Anything that maps onto criminal activity, e.g. pornography)
To monitor terrorist activity; (accept two different types of each category)
To monitor political groups; (accept two different types of each category)
A To monitor for viruses which threaten economic wellbeing of country or have a criminal intent;

2

(b) One way: encrypt content;
A encode/send in code

1

[3]

Q30.

Ill trained/ inexperienced users
Fire/Explosion
Burglary
Hardware Failure
Software Failure
Viruses
Hackers
Disgruntled Employees

Any 3
1 mark for each risk + 1 mark each suitable defence

[6]

Q1.

Around half of students achieved some marks for this question, but full mark responses were seen very infrequently. Good responses recognised issues such as the fact that the Internet crosses borders but laws typically relate to only one country or that technology changes very quickly so it is difficult for legislation to keep up. Some students just listed Acts of Parliament in the UK rather than addressing the challenges and a minority did not understand the term legislator, believing a legislator to be an employee of a company.

Q2.

Although many students achieved at least some marks in this question part, few showed the depth and breadth of understanding required for the highest marks. Some students appear to have answered the question provided in the specification rather than this question, possibly because both featured Google Street view. Unfortunately, because the questions were significantly different this led to few if any crossover marks and highlights the importance of reading questions carefully. Other students referred to the service entering private homes or being based on public streets. These did not receive marks unless the concern was still relevant for the context given. Stronger answers looked in depth at all aspects of the question but did not go into too much depth about each point – those who did tended to repeat themselves and receive limited marks for extended sections of writing.

Although specific laws are not on the specification, a number of students referenced acts such as the DPA, CDPA, etc. In these cases, a significant lack of understanding was shown, where students are taught about the acts, it is encouraged that sufficient levels of understanding are ensured so as to not inadvertently contradict themselves and hence lose marks.

Q3.

This question required students to write an extended response that covered a number of different areas of the specification. Responses often covered the aspects of how the owners could have protected their networks and what legal and ethical issues might have arisen well but neglected the aspect of how it was possible for the data to be collected and were not specific enough with regard to how the company's practices might have changed as a result of the incident.

With regard to how the data was collected, examiners were looking for students to recognise that WiFi signals could travel over a wide area and that any WiFi receiver in range could read the data from these packets. Few students made these points, but a reasonable number identified that the data may not have been encrypted or that an outdated encryption protocol such as WEP might have been used.

Good responses recognised that an appropriate measure to prevent the data from being collected would have included encrypting the data using a protocol such as WPA2. In the question's context, measures such as enforcing a MAC address whitelist or using a firewall were not appropriate as the cars were simply collecting information that was being transmitted; they were not trying to connect to the wireless access points. Some students referred to adding a password to the network which was not a strong enough point to be mark worthy; they failed to identify that the "password" they were referring to would actually be used to make a key for an encryption system.

Students are not required to have knowledge of specific legislation for this specification,

but should have an understanding of issues around areas of ethical and legal concern such as privacy, data protection, copyright and hacking. Nevertheless, mention of specific relevant legislation was considered mark worthy. Relatively few students took the opportunity to really discuss the legal and ethical issues. For example: given that the data was being transmitted freely through the air, would accessing it really count as hacking, given that the functionality involved was added by a small number of developers, were they or the company responsible for it, would the nature of any offences committed depend upon the type of data collected, did it matter if the data collection was intentional or accidental? Students should be encouraged to consider this sort of reflection when answering this type of question.

Most students recognised that the company needed to have better oversight of the development process but many made general statements about this and did not suggest specific measures that might be taken to improve their practices, such as introducing third-party review of code or improved training of developers on legal and ethical issues. Points relating to testing were not considered mark worthy unless it was explicitly stated that the testing would be focussed on ensuring that the software had no additional functionality or that the data collected by the cars was all relevant to the intended purpose of the system.

Some students appeared to have completely misunderstood the scenario and wrote at considerable length about the rights and wrongs of companies using cars to take photographs in public places rather than about interception of WiFi signals. Students need to ensure that they are answering the question asked rather than a question that they might have prepared for.

Q4.

Providing two important aspects of a robot was answered well by students and the majority secured one mark if not two. The most common answers included the idea that a robot is programmed and that it can sense / respond to its environment.

The question about computers and intelligence provided an insight into students' understanding of this area and proved interesting to mark. A group of students could link answers into ideas such as Moore's law, the Turing test and the Chinese Room argument but these were not necessary to gain marks as they are not part of the specification. This evidence of knowledge around the topic continued with students providing examples of where intelligence might already be represented with Asimov, Watson and chess playing devices such as Deep Blue.

The commonest idea as to why computers might become intelligent was the continuing advance of technology. For the students arguing that computers will never be intelligent, the main points were around the idea of the restriction of being stuck in a program and the lack of creativity, emotion and 'thought'.

This question then continued with parts about hacking and it was clear that students had some understanding of this area. Identifying the Computer Misuse Act was done well by the majority of students. It was also pleasing to see the answers provided for part (c)(iii). Good answers pointed out ideas such as VPNs and masking IP addresses. The use of botnets was also described by some students. The answer of 'leaves no traces' was not rewarded a mark unless a student provided more detail.

Q5.

(a) This part was answered well by the majority of candidates. It is evident that candidates can link a piece of legislation to a given situation. The legislation that caused a few candidates to stumble was the Regulation of Investigatory Powers Act

and how this could apply to a request to hand over an encryption key.

(b) This part was based around the context of having a system for taking car park charges through the use of CCTV and mobile phones. It is important for candidates to keep in mind the context of questions when answering as it was common to see very general points made whilst better answers were clearly tied back to the context.

(i) This part of the question came out harder to answer than expected. Around a quarter of candidates responded with the correct answer of optical character recognition. It was evident that a lot of candidates did not know what OCR stood for and we saw a variety of imaginative responses.

(ii) This part has been asked before on previous papers but candidates did struggle to secure the mark this year. We are looking for personal data to be about a living person who can be identified from that data. A few candidates did not secure the mark because they missed out the distinction that the person must be living. Weaker candidates just provided examples of personal data.

(iii) This part of the question was looking for candidates to use the context of the question to provide some reasons for privacy campaigners to be concerned about regarding this system. It was pleasing to see that a group of candidates could identify that the data stored might have the potential to be used to track the location of people. Another common and accepted answer was that the data could be sold on and then the mobile numbers could be used for cold calling. The idea of data not being kept securely was also a valid response and secured a mark.

Q6.

The majority of students correctly identified that the first part of this question concerned the Data Protection Act. Students did struggle, however, to identify the principle required for part (b) and then to name another for part (c). It was common to see statements about certain activities for protecting data rather than stating actual principles. Part (b) was looking for the idea of data security and some students correctly identified the difference between internal and external security. The common answers for part (c) included keeping data up to date and not keeping data longer than necessary.

The majority of students correctly identified that HTTPS would be the preferred protocol for transmitting this data and over 60% secured the second mark for this question part with the common answer of HTTP not being a secure protocol. There appears some confusion over what HTTPS actually is and answers such as ‘the website could be hacked’ or ‘the website is not secure’ did not gain marks. At this level we would encourage students to appreciate that HTTPS is a protocol involving the encryption of data transmitted between two devices for the purpose of making the transmission secure but the protocol doesn't imply that all of the data on a website is actually secure.

Part (e) was answered well by students with the majority scoring 2 or 3 marks. Mistakes included identifying the web server software as either an operating system or a utility program. It seems possible that students do not have experience of servers and how they operate.

Q7.

For part (a) a few students missed a mark by not providing the full name of the law, but the majority did achieve this mark.

Students provided a variety of good reasons for parts (b) and (c) and it was pleasing to see their understanding of this topic. Many students talked about the loss of income for artists and retailers if music was available free. Quite a few students linked this into the failure of businesses and highlighted HMV as a recent case. As this question part was considering music files the idea that they could contain a virus or spyware was not awarded any marks.

The question part about the availability of DRM-free files allowed many students to pick up a mark by identifying that this has the advantage of being able to place the files on multiple devices. The idea of always needing an Internet connection was not awarded a mark for this paper but it was noted that this is how DRM can work for gaming files.

A few students did not quite understand that copyright might still be part of a DRM-free file; whilst there is no technology to limit the use of the files they still would be covered by the idea of copyright.

Q8.

Part (a) of the question started by asking students to identify a use of a collection of protocols. The majority of students could correctly identify a use for FTP and it was obvious that this was a well known protocol. Students, however, struggled with both Telnet and POP3. Whilst the majority of students knew that POP3 was concerned with e-mail, this was not considered to be creditworthy as students should be aware of the difference between POP3 and SMTP. Students who did identify that POP3 was concerned with retrieving e-mail from a server were rewarded with the mark. It would be beneficial for students to have access to working with these common protocols so that they can gain a feel of their use.

The first few parts of (b) were answered well by students. Most secured the mark for IP address and port, but providing a socket came out as the hardest of the three parts. The most common incorrect answer for port was 37 with students picking this out from a different column of the figure. In a similar fashion, it was common to see a variety of items taken only from the figure as a guess at socket.

The last part of question was answered well with the majority of students gaining at least one mark. A wide variety of answers were seen across the marking period. Popular answers included the servers being off-site and the point that it would save time being able to access the servers from a desktop rather than travelling to them. Students who realized that the servers might be able to be managed from anywhere with an Internet connection were also awarded a mark.

Q9.

This is the first time that students have been asked to consider the Health and Safety legislation. It was pleasing to see that the majority of students could identify the law and a good number managed to secure all of the marks.

Students need to read questions carefully as although companies do need to provide eye checks to employees who use monitors this would not affect the design of the workspace. A small group of students also thought this question concerned the Data Protection Act and provided ideas concerning making sure that screens could not be viewed from a distance.

In previous papers we have referenced the Copyright, Designs and Patents Act, yet only around 40% of students correctly identified it again in this paper. Some students failed to secure the mark as they did not state the full name of the law as was asked.

The majority of students did secure the mark for the next part and it was pleasing to see the variety of correct answers. Most students wrote about checking how many computers the software could legally be installed on or considered the type of licence that the library might have.

The majority of students secured the last mark in the paper by correctly identifying what a Code of Conduct is and, as this question part has been asked before, it is probably a topic that is well known.

Q10.

Students generally scored very well when completing the table of different storage media. Students who dropped marks tended to place CD media into the 3GB row and therefore not appreciate fully the different storage capacities.

When describing the workings of a CD drive it was clear that the majority of students appreciate that it uses a laser to read and write the data. To secure two marks, however, students needed to differentiate between the power of the laser being used in the read and write processes. Students who clearly described the difference on the physical media to represent binary 0s and 1s picked up the mechanism mark. Weaker students provided answers along the line of, 'pits store 0s and 1s,' and did not distinguish between pits and lands. A minority of students continue to mix up optical and magnetic media and wrote about magnets being used to write or read data. A few students described needles being used to scratch data onto the disk perhaps remembering vinyl records.

Question part (c) was generally answered well with the majority of students securing at least one mark. The most common answer was along the lines of the CD becoming damaged or scratched. Students need to be aware, however, that to gain a second mark they need to identify a different point from the first. A CD becoming scratched and a CD becoming damaged are not different enough to secure two marks. Students who recognised that the file format might no longer be supported secured a mark. There was slight confusion for a few students who stated that a DVD drive would not be able to open a CD.

Q11.

Whilst most students provided answers for part (a), it was quite common to see the stem of the question simply repeated. The answer, 'an ISP provides an Internet service,' was not enough to secure a mark. Students secured the mark by describing how an ISP supplies a connection or access to the Internet to their clients.

It is usual for question papers to now ask students to state the full name of a law and a few students lost marks in question by not following this instruction.

The answer of simply, 'copyright,' is not enough to secure a mark and this led to around half of all students securing a mark for part (b).

The term 'personal data' has appeared on past papers and it is still evident that students struggle to define this well enough to secure the mark. We are looking for personal data from which it is possible to identify a living individual.

Question part (d) asked students to identify two further laws and the majority of students secured both marks. More students secured the mark for identifying the Data Protection Act over the Computer Misuse Act. Occasionally students answered with 'Data Misuse Act' or 'Computer Protection Act' which perhaps identifies that they have heard about the laws but are not able to state the names correctly.

Q12.

Question allowed students to provide many varied answers and the majority of students managed to secure some marks. Most students identified that the spraying of car bodies is a repetitive task and stronger students then discussed this as being in a controlled environment with little deviation to a set routine. The automatic car control did fire up students' imaginations but some did not link this very well to how computers and robots work. Stronger students identified the need to measure many inputs and the variety of sensors needed. Students who described the environment as unpredictable also secured a mark.

Q13.

The answer for part (a) has been asked before and candidates should be aware that we are after the full name of the law. Many candidates stated only 'copyright' and did not secure the mark. The actual law is the Copyright, Design and Patents Act.

Digital Rights Management has also been asked about before, but many candidates did not secure any marks for part (b). Many candidates answered by stating that DRM prevents one from copying the file, rather than preventing playback if a file has been copied. Discussion about limiting the number of times a file could be played or placing a time restriction onto the file did not secure any marks as this would not stop the sharing of downloaded files which was the point of the question. Candidates need to make sure that they answer within the context of the question. Some candidates answered by stating that it was illegal to share copyrighted files or that, terms and conditions would have to be agreed. Both of these points might be true, but it does not stop the sharing of downloaded files. The usual correct answers were the 'file being encrypted' and 'playback being limited to one device'.
Candidates sometimes wrote about passwords, codes or PINs to playback the file, rather than the correct answer of a decryption key.

Q14.

Question provided a variety of answers with candidates generally scoring quite well. Many candidates identified machines as being good at precise and accurate actions and being able to repeat these whilst not growing tired or needing breaks. The candidates who mentioned machines being good at calculations only secured the mark if they expanded to talk about complexity or gave a complex example.

Candidates who stated only that machines can perform dangerous tasks did not secure a mark unless it was expanded or made clear that humans would find them too dangerous. Many humans are also involved in dangerous tasks.

Candidates found it harder to describe what machines are bad at, but those who stated that machines cannot think for themselves were awarded a mark. Better candidates wrote about a lack of creativity or inability to respond in unexpected circumstances. Candidates should be aware that machines can sense their environment and make decisions; however it is unexpected circumstances that cause machines problems.

Q15.

This question asked about robotics from a different point of view from previous papers. The two parts were clearly linked and reasons given in the second part had to relate to the task identified in the first. On some occasions candidates gave general reasons for why a robot might be used that did not relate to their example and so did not gain credit. Others gave examples that were not suitable for completion by robots and so lost all of the available marks.

Q16.

This is the question that also concerns quality of English and was asked around DRM (Digital Rights Management). The ideas about protecting copyright / preventing copying and ensuring artists get paid for their work were well known as were the opposite ideas of problems making legal backups, and not being able to play the items on a range of hardware / software platforms.

Many answered a different question i.e. how DRM works. There were many references to the fact that DRM infringes human rights! This was another example of some candidates not reading the question as many answered with reference to software rather than music / video DRM.

There were many answers arguing that using DRM puts up the cost of the purchased media but this was usually stated in a vague manner. There was also much philosophising about theft and 'right and wrong', but candidates often stated that if you could not afford it (the music or video) then you should get it for free.

Q17.

Part (a) was about legislation. Candidates often gained full marks. The most common answer was the Data Protection Act in subparts (i) and (ii). Again some candidates appeared to be answering questions set in the previous year's paper. Small errors in the name of the legislation were ignored which did make it easier to obtain the marks in these components. Subpart (iii) was the one that was most often left blank.

Part (b) was about a Code of Conduct. Subpart (i) challenged the candidates' ability to explain / describe what was expected. It was often clearly stated that a Code of Conduct was a set of rules but the need for employees to follow it or be bound by it was less frequently stated and so this point was lost. Very rarely did candidates mention that this was a documena contract (written document) and that its contents did not necessarily constitute a legal requirement.
Subpart (ii) was answered in much vaguer terms than (i). The most frequently seen correct answer concerned the ability of the company to take disciplinary action against employees who had signed the code of conduct.

Q18.

The Data Protection Act defines Personal Data as, 'Data which relate to a living individual who can be identified ... from those data.' Many candidates had clearly learned this definition and were able to state it accurately. Some, however, gave very general answers such as, 'data about a person,' or, 'data that people would not want others to know,' that were not worthy of credit.

Many candidates were able to state a principle of the Act that could be met through careful design of the program. The most frequently cited principles were that data should be kept securely and that data must be kept up to date. Some candidates mistakenly stated measures such as password protection or backing up data, rather than principles. Most candidates who were able to state a principle of the Act were able to identify an appropriate measure to ensure the principle was met and explain how this occurred.

Some candidates had learned short phrases to help them remember principles such as Quality, Lifetime and Security, but stating these alone was insufficient. Quite a lot of candidates held the mistaken belief that data could not be given out to anyone.

Q19.

Most candidates understood that the purpose of DRM was to control access to digital media, so as to prevent piracy. Fewer went on to explain that this was done to enforce copyright legislation and to ensure that artists received the income from music sales. Some errantly believed that DRM was a law or a company.

Many candidates were able to explain at least one method of applying DRM, the most common descriptions being of encryption or limiting playback to a particular hardware device or piece of proprietary software. A common, but incorrect response was that DRM could stop the music files being copied, whereas DRM is unlikely to be able to do this. Rather, if the files are copied they could not be played. Some candidates mistakenly continued with their descriptions of why DRM was used or gave advantages and disadvantages of it, rather than explaining how DRM would work. Encryption and encoding are not the same things, nor are a key and a code or password.

Q20.

Even candidates who illustrated their answer with a suitable application such as car manufacture or bomb disposal found it exceedingly difficult to describe what is meant by a robot. The description needs to distinguish the system from a standard desktop computer running sophisticated software. A robot is a mechanical structure that can make dextrousmovements, is programmable and has some degree of intelligence to sense and react to its environment. Robots are used because they can perform repetitive tasks that require precision and produce consistent quality, even during continuous operation.

Q21.

Part (a)(i) of this question was asking how, in a large system, access could be restricted so that staff could only access those parts of the system that they required to carry out their job role. More was expected than just ‘password protect’, or ‘have user names and passwords’. The use of passwords was relevant, but for full credit, candidates had to also say, for example, that passwords should be chosen so they would be difficult to guess, or should be changed regularly. Other suggestions which gained credit were for the use of access rights or attributes to restrict access to particular users or user groups, or to restrict access to certain files to certain terminals with methods of then restricting access to those terminals. Another acceptable suggestion was to encrypt sensitive files with only authorised users having the decryption key. Several candidates assumed that ‘online’ meant a website and not simply access to data stored in digital format on a computer system. This slightly changed the way they responded.

For part (a)(ii) the question was how to detect illegal entry, not how to prevent it, so locking a workstation after 3 incorrect password attempts did not answer the question. Several candidates understood the concept of logging or monitoring users via system/network software, but just as many implied that tracking was physically done by the network manager, that someone was employed to watch the monitors of users or that it was files that were logged. The use of CCTV was not considered appropriate in this case.

In part (b), candidates needed to answer carefully to gain marks. A firewall might prevent hackers but for a virus checker to be effective if it had to be regularly updated and used. Similarly backups need to be taken regularly to be useful in the event of a system crash. Instead of knowing what a UPS is, students preferred to mention ‘backup electricity supply’ and backup generator. However, current generators do not provide a constant nor uninterrupted supply of power; there is a still a short time of switch over when there is no power supply.

Sadly, some candidates did not read the word ‘further’ in the stem of part (c), and repeated something about using back-ups for swift restoration. However, there were many

good suggestions for this, including the description of a recovery procedure and the use of contracted out recovery.

Q22.

This question was generally done well. However, few candidates saw the significance of the radio-frequency remote control. Answers worthy of credit needed to highlight the usefulness of this device over other remote controls which require the control to be in line of view of the device to be controlled. Very few candidates could suggest any use for a programmable switching unit, often expecting the user to sit at a computer to control this unit, rather than the expected answer of pre-programming the switching of lights/heating/multi-media etc according to times of day/week.

The reasons given for using any of the components was often just re-iterating the question stem (the client cannot stand easily and has limited use of their arms). Candidates need to be reminded that this will not gain credit and that further explanation is expected, such as a wheelchair user may find it difficult to open windows as they find it difficult to reach handles and push/pull.

Q23.

Candidates had to explain different social, economic and ethical consequences of spam. A certain degree of freedom was accepted in distinguishing between social, economic and ethical consequences as it was appreciated that there is frequently an overlap between these three categories. However, some candidates did give the same answer for two categories, and were not credited for both.

For the first time, this paper was e-marked, and it is intended for this to continue. The scripts are scanned into a computer system and examiners see the scanned clips on a computer monitor and mark these. It would therefore be helpful if candidates for CPT2 papers write their answer in blue or black ink because this scans well.

Q24.

A response that gained credit for part (a) was 'the rights of the software owner to control how the software is used, copied and distributed'. Although many candidates defined a license rather than copyright, most candidates made a good attempt at what could and could not be done under the terms of a license for parts (b) and (c).

Q25.

For an answer to this question to be credit-worthy, candidates had to be clear who exactly was benefiting in each case. For part (i) the beneficiary had to be the Universities, who would gain revenue and respect from this scheme. In part (ii) the benefits were mainly economic as students could remain at home, possible working while studying. It would also benefit students on the move as they could continue their studies anywhere in the world, and regardless of time zone. In part (iii) it was the businesses, not their employees whose benefit was sought, so the fact that employees could continue to pull their weight at work, could apply their knowledge to their work immediately and would be more skilled, motivated and effective were all good answers. The most common reason for lost marks was that some candidates answered all three parts from the student perspective.

In order to study in this way, students would need a modem or other connection to the Internet, and they would need a browser, communication software, and possibly bulletin board software and the online teaching software. Here again, brand names were not credited.

Q26.

Candidates were able to identify a benefit to the user such as *additional information not recorded on CD cover may be available from the software company* or *information related to user interests could be supplied*. However, for a benefit to the software company, many candidates failed to supply enough to gain a mark. Targeted marketing was often identified without relating the marketing to saving of costs or the generation of extra revenue.

Part (b) was well answered with many candidates quoting “invasion of privacy”.

Q27.

Candidates performed well on this question.

Q28.

In part (a) most candidates realised the need for round the clock availability because of countries being in different time zones. In part (b) many candidates offered answers that lacked perception and therefore failed to gain credit. “Encryption stops hackers accessing messages” was a popular answer that gained no credit. Credit was given for answers that gave the consequences of being able to read an unencrypted message, such as being able to retrieve information for fraudulent purposes.

Candidates were less successful at reasoning why governments require banks to lodge encryption keys with them. Few answered correctly “so that governments can track money transfers made by criminals or terrorists” whilst many candidates simply stated: “so that governments can monitor messages” thus falling short of what was considered creditworthy.

Q29.

Many candidates correctly identified to monitor criminal activity and to monitor terrorist activity. Some candidates answered quoting a specific example, “to catch paedophiles at work exchanging child pornography”, which also gained credit.

Several candidates answered that the reason was “to look out for viruses” which was not quite enough to gain credit. Those candidates that answered more fully “to detect and prevent viruses from causing economic harm to the country” did gain credit. Often a candidate’s response to a “give reasons” type question falls short of the expected answer because the detail is missing. “To look for criminals” would not be enough whereas “to look for criminal activity” would be.

The majority of the candidates gave the creditworthy answer ‘encryption’ as their response to part (b). A few wrongly suggested using a password.

Q30.

A high scoring question but a clear preference for hackers and viruses. A large number of candidates were unable to come up with a third threat.