STOKE DAMEREL
Community College

Cycle 2

IT

Year 11

Name: _____

Tutor: _____

Year 11 Homework Timetable

Monday	English	Ebacc Option A	Option C	
Tuesday	Tassomai	Option B	Option D	
Wednesday	Hegarty	Science	Option C	
Thursday	Ebacc Option A	Tassomai	Option B	Option D
Friday	Hegarty	Science	English	

Tassomai - 50 questions per week
Hegarty - 4 tasks of Hegarty per week

Block A	Block B	Block C	Block D
French	Art	Art	Business Studies
Geography	Business Studies	Business Studies	Catering
History	Child Development	Catering	Dance
Sociology	Catering	Drama	Drama
	Computer Science	History	Geography
	IT	Music	Media Studies
	Media Studies	Photography	Photography
	Sociology	Sport	Sport
	Sport	Travel & Tourism	

Aspire | Achieve | Thrive

GREENSHAW LEARNING TRUST

Year 11 IT
Cycle 2

Week Number	Homework Task	Exam Question
1 **15th November**	**Cornell Notes** User Access Restrictions	Open Wifi Networks
2 **22nd November**	**Cornell Notes** ● Data Level Protection ● Finding Weaknesses in IT Systems	Firewalls
3 **29th November**	**MOCK EXAM WEEK** Ensure you revise thoroughly for your MOCKs	
4 **6th December**	**MOCK EXAM WEEK** Ensure you revise thoroughly for your MOCKs	
5 **13th December**	**Cornell Notes** ● Defining Responsibilities ● Disaster Recovery	Password Policies
6 **3rd January**	**Cornell Notes** ● Shared Data	Using Cookies
	Cornell Notes ● Environmental Concerns	Environmental Factors
8 **17th January**	**Cornell Notes** ● Equal Access and Net Neutrality ● Acceptable user and Boundaries ● Data Protection	Net Neutrality
9 **24th January**	**Cornell Notes** ● All topics	

Week 1: Prevention and Management of Threats

Firewalls - Monitors incoming and outgoing network traffic and blocks suspicious packets based on security rules. Can be a piece of hardware (physical device) to protect the network or software (computer program) installed on every device on the network. Often hardware **and** software firewalls are used (as they provide protection in different ways).

Anti-Virus Software - A piece of software that can scan for and remove malware (viruses, worms, trojans, spyware, rootkits, etc). Will usually offer 'real-time' protection which scans files as they are downloaded or opened.

Interface Design - Designing the User Interface to provide security. This can include obscuring data entry (******** for passwords), autocomplete so users don't need to enter data (which may be picked up by a keylogger), stay logged in option to prevent users having to sign in every time (prevents shoulder surfing - someone looking at another user typing their password).

Firewalls		Anti-Virus Software		Interface Design	
Benefits	**Drawbacks**	**Benefits**	**Drawbacks**	**Benefits**	**Drawbacks**
Prevents external attackers from gaining access to your computer system by blocking their attempts. Usually very cheap to install and set up software firewalls. Most operating systems come with them built-in.	Firewalls can be restrictive, preventing employees from performing legitimate activities, like visiting certain websites. Software firewalls take up resources and slow computer & network performance. Hardware firewalls could slow internet speed.	Prevents all forms of malware from ever infecting your computer system. Usually reasonably affordable and relatively simple to set up.	It must be regularly maintained and updated. Otherwise it won't detect some malware. Running a scan can be resource intensive and lead to your computer running slowly.	Good design can reduce the need for overly stringent security measures.	Focusing on security may sometimes worsen ease-of-use & accessibility.

Week 2: Backup and Encryption / Identifying Weaknesses

Backing Up Data - You should take regular backups. How regular depends on your business, as for some a weekly backup is fine, as they don't do much business on a daily basis. Some might need hourly backups though. Generally, daily backups are common. Backups should also be stored in a remote location. This means they're stored somewhere other than where the original data is. This way, if your building burned down or flooded, your backup won't be affected. It is quite common to use cloud storage for remote backups.

Encryption - This is the process of converting plain-text data into an encoded form known as ciphertext. This ciphertext is unreadable until it is decrypted. We encrypt data using an encryption algorithm and an encryption key. The algorithm is the process performed to convert the data into the ciphertext. The key is a unique string (combination of letters and numbers) that is applied to the algorithm to ensure the encryption output is unique (so someone using the same algorithm but a different key will get different ciphertext output). We most commonly think of encryption when we are transmitting data, such as when we send our bank details to an online shopping website over the internet. However, we sometimes encrypt stored data too.

Finding Weaknesses. Weaknesses in computer systems can be identified through three strategies:

- Ethical hacking – An individual or group who purposefully uses techniques such as penetration testing & social engineering to identify weaknesses in a system to help prevent future malicious attacks. There are two common forms of ethical hacking:
- Penetration testing – A process used by cybersecurity professionals in order to identify security vulnerabilities in a computer system. This can involve techniques like port scanning, vulnerability scanners & packet sniffers to identify weak points such as open network ports, coding flaws, out of date software & missing encryption.
- Analysis of system data/behaviours – The process of observing a system's data and its users' actions in order to assess whether the data is being held securely and whether it can be accessed in some way. This might identify a weakness, such as users taking confidential data out of the business to work at home.

Week 3: Policies to protect data

Defining Responsibilities

To implement and maintain cybersecurity policies, companies will assign specific roles to IT staff or management. This allows for accountability and ensures staff are constantly aware of the actions they need to take.

- Roles / responsibilities – A member of the IT staff or management will be responsible for deciding what policies must be put in place. It's important that specific employees are assigned responsibilities for implementing these cybersecurity policies, usually members of the IT staff.
- How to report concerns – There should be clearly defined the person that staff should contact if they have a concern over a possible incident or poor practice. This is commonly the individual(s) responsible for implementing and maintaining the policy.
- Reporting to staff/employees – Security policies are only secure if staff are aware of the policy and its procedures. There should be someone responsible for making staff aware and training them on following the cybersecurity policies put in place.

Setting Policies

Your cybersecurity policies will define security parameters (rules / guidelines) that must be implemented and maintained to protect the business from harm caused by an incident. These parameters might include the following:

- Password Policies - How to create safe, secure passwords (eg 8 characters minimum, mix of upper / lower case / numbers, etc). Also, how to keep your passwords safe and secure (not sharing with others / not writing them down, etc).
- Acceptable Software Policy - Used to control what software can be installed on a computer system. This prevents user accidentally downloading a virus or downloading software that may conflict with other programs on the system. Some users may be blocked from installing software altogether.
- Acceptable User Policy - An acceptable use policy defines what a user can and cannot do on a company's IT systems. The purpose of this policy is partially to prevent employees from wasting time, such as by playing video games or using their personal email during company time. However, another major reason behind it is to keep company IT systems safe from threats.

Week 4: Shared Data (You should also recap Week 1 this week)

Collecting and Use of Shared Data

Companies collect data shared to them by their customers, and this data can then be used for a variety of purposes including advertising, planning, and providing services.

- Location-based-data – sharing location data is encouraged increasingly by websites and mobile apps. Especially with the growth of mobile devices with GPS that constantly logs our location. This is then used for all kinds of purposes. Some websites might show you country-specific deals, some to show you where to find restaurants local to you, some to help you plan a route on a map.
- Transactional data – Every time a purchase is made, a record of this is stored. This might include the time, date & cost of the transaction and the item purchased. This is used to customise advertising to you, analyse buying habits, track stock levels and identify trends in sales.
- Cookies – Most browsers collect cookies to carry data between the times you visit a website, such as leaving you logged in, or remembering settings like a language preference. It can also be used for analytics, like tracking how long you spend on a page. This can be used to improve the ease-of-use, customise advertisements & analyse website performance.
- Data exchange between services – data collected can sometimes be shared with another service. This might be one app sharing data with another. For example, your smartphone will gather data on your location, this can then be shared with Facebook, Google Maps and many others. Many apps and websites will exchange the data they gather (though they have to ask your permission).

Benefits and Drawbacks of Shared Data

Benefits	Drawbacks
• Shared data allows us to access large datasets for analysis. This means we can make better decisions. • Allows companies to target information better for you, making their services more useful and easier to use. • Shared data helps companies to advertise more effectively, by using data gathered to personalise marketing. • Shared data saves you from having to collect all of the data yourself. This will save time and money.	• Data cannot be shared without the permission of the user. Otherwise you may be fined under the DPA. • If sensitive, data may be intercepted in transit and misused by a malicious user. • Shared data may not be accurate or may contain malware which will harm your systems. • Sharing data may be seen as an invasion of privacy & upset some customers.

Week 5: Environmental Concerns (You should also recap Week 2 this week)

Environmental Impact of IT Systems

The environmental impact of IT systems isn't just the electricity used when running IT systems. It occurs during all stages of the life of an IT system. For example:

- **Manufacturing** - Sourcing raw materials (including materials, such as copper, gold and silicon) | Electricity and gas required to power factories, which produces harmful emissions | Fuel to transport IT systems to businesses / shops for resale.
- **Use** - The electricity to power and charge devices | Wasted electricity from leaving computers switched on when not in use.
- **Disposal** - When technology is no longer needed or out-of-date, it is often thrown out (not always recycled).

Upgrading versus Replacing

Do we upgrade a computer system by upgrading its components or do we replace it completely and throw away the old system?

Benefits	Drawbacks
• It's cheaper to upgrade IT systems rather than replace them. • Upgrading will produce less waste that will end up in landfill.	• Quicker for a business to buy a new system than upgrade. • New technology may adhere to stricter environmental standards, with better energy efficiency / less power used.

Usage Settings

We can reduce the impact that our computers have on the environment by changing how we use our computer systems and the settings we configure them with. Some of these settings include the following:

- Auto Power-Off – Most devices have power-off settings that place your device into a standby state, or completely turn off, if it has not been used for a certain period of time. This will save on the wasted energy when we leave our computers on when not in use.
- Power-Saving Settings – Most devices also have settings for reducing the power consumption of a device. This might be by lowering screen brightness, turning off wireless connection methods like Bluetooth, certain features might be turned off & even reducing CPU speed. This will save on the amount of energy used while the device is in use.
- Electronic Distribution – Distributing electronic files rather than physical printed copies will save on wasting paper which will help reduce deforestation. We can also use digital downloads instead of purchasing physical software to reduce the environmental effect of distribution (pollution from planes and lorries).

Week 6: Cyber Defenses (You should also recap Week 3 this week)

Computer Systems can be protected in a number of ways:

Physical Security - Locks, alarms, guards, CCTV	Passwords (including PINs and 'gesture passwords')	Biometrics (fingerprint, facial or voice recognition)
Testing - using ethical hackers and penetration testing to check for flaws in a computer system and fixing them.	Two-factor authentication - user provides two forms of identification. Eg. password **and** voice recognition.	Device hardening - updating devices, installing security updates, using encryption to scramble data.
Firewalls - to monitor incoming and outgoing data and blocking suspicious activity.	Anti-virus software - to check for and remove malicious software from a computer system.	Backing up - keeping copies of data in case an attack takes place.

Week 7 and 8: Preparing for Assessment

Self-quiz the knowledge covered in Weeks 1 - 6

WEEK 1

Date……

Mina works for a computer network installation company. He designs and installs computer networks. Mina works remotely.

When Mina is installing networks he uses open wi-fi networks to access data.

Explain two possible external security threats to Mina when using open wi-fi networks.

[4 marks]

Answer:-

WEEK 2

Date……

Buyable Crafts is a company that makes and sells craft items. It uses its own designs for the items. Buyable Crafts stores customers' personal details on its systems.

It must abide by UK legislation governing data protection. Buyable Crafts must protect the data that is kept on its system.

One way to do this would be to use a firewall. Describe how a firewall can protect this data.

[4 marks]

Answer:-

WEEK 3

Date……

A doctor's surgery provides medical care for people in the local area. The surgery uses Information Technology to collect, store and process patient data.

The surgery manager will create a password policy for staff. Changing passwords regularly is one rule they will include.

Give **two other** rules they could include in this policy.

[2 marks]

Answer:-

WEEK 4

Date……

A company sells vegan food and clothing. It has decided to create a website to sell its products.

The company uses cookies on its website to help improve business.

There is UK legislation that governs the use of cookies. Explain **two** rules the company must follow when using cookies on its website.

[4 marks]

Answer:-

WEEK 5

Date…….

An online company designs and sells gadgets. The company wants staff to use digital systems responsibly.

Discuss how staff can use digital systems responsibly to help protect the environment.

[6 marks]

Answer:-

WEEK 6

Date…….

TechnoWhizz is a technology development company based in London that makes a range of digital systems, devices and apps.

TechnoWhizz wants to introduce a video streaming service to provide content for their devices.

Describe how 'Net neutrality' will help TechnoWhizz compete with more established video streaming services.

[3 marks]

Answer:-

STEP 2: CREATE CUES

What: Reduce your notes to just the essentials.

What: Immediately after class, discussion, or reading session.

How:

- **Jot down key ideas, important words and phrases**
- **Create questions that might appear on an exam**
- **Reducing your notes to the most important ideas and concepts improves recall. Creating questions that may appear on an exam gets you thinking about how the information might be applied and improves your performance on the exam.**

Why: Spend at least ten minutes every week reviewing all of your previous notes. Reflect on the material and ask yourself questions based on what you've recorded in the Cue area. Cover the note-taking area with a piece of paper. Can you answer them?

STEP 1: RECORD YOUR NOTES

What: Record all keywords, ideas, important dates, people, places, diagrams and formulas from the lesson. Create a new page for each topic discussed.

When: During class lecture, discussion, or reading session.

How:

- **Use bullet points, abbreviated phrases, and pictures**
- **Avoid full sentences and paragraphs**
- **Leave space between points to add more information later**

Why: Important ideas must be recorded in a way that is meaningful to you.

STEP 3: SUMMARISE & REVIEW

What: Summarise the main ideas from the lesson.
What: At the end of the class lecture, discussion, or reading session.
How: In complete sentences, write down the conclusions that can be made from the information in your notes.
Why: Summarising the information after it's learned improves long-term retention.

Date / / **Topic** **WEEK 1**

Questions	Notes

Summary

Date / / **Topic**

Questions	Notes

Summary

Date / / **Topic** **WEEK 2**

Questions	Notes

Summary

Date / / **Topic**

Questions	Notes

Summary

Date / / **Topic**

WEEK 3

Questions	Notes

Summary

Date / / **Topic**

Questions	Notes

Summary

Date / / **Topic** **WEEK 4**

Questions	Notes

Summary

Date / / **Topic**

Questions	Notes

Summary

Date / / **Topic** **WEEK 5**

Questions	Notes

Summary

Date / / **Topic**

Questions	Notes

Summary

Date / / **Topic**

WEEK 6

Questions	Notes

Summary

Date / / **Topic**

Questions	Notes

Summary

Revision Page

Revision Page

Revision Page

Revision Page

Revision Page

Revision Page

Revision Page
