Holy Family Catholic High School

Subject	Year	Term
WJEC LEVEL 1/2 VOCATIONAL AWARD IN ICT	**11**	Spring

Topic
1.3 Legal, moral, ethical, cultural and environmental impacts of IT and the need for cybersecurity

Content - Intent	
Prior Learning (Topic)	Key Stage 3 National Curriculum
Learners will have a basic understanding from KS3 about a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns.	
Future Learning	Revision for Unit 1 examination

What Knowledge and Skills will be Taught (Implementation)	How will your understanding be assessed and recorded (Impact)
1.3.1 Risks to information held on computers Learners should know and understand about accidental damage, unintended disclosure by incorrectly assigned access levels and malicious software including viruses, worms, Trojan Horses, spyware, ransomware, DDoS and key logging. This topic will also explore hacking (e.g., white, black and grey hat), social engineering and emerging threats in the modern world.	Learners should be aware of how they themselves could accidentally lose data, as well as understanding threats from outside of their system, which might include malicious software, hacking and social engineering. This section will enable learners to understand the importance of backing up work, sharing personal details in limitation and only when necessary, having different security passwords for different uses/platforms and so on. Beyond the concept of hacking, learners will be introduced to the concept of ethical hacking and penetration testing in order to develop an understanding of how companies deal with threats to data and privacy. Learners should also be aware of a range of common attacks, alongside emerging threats, as these are the ones they are likely to face in the workplace. This will help learners to be vigilant and keep their information safe. It is only by being aware of these risks that learners will be able to take steps to prevent data loss. Learners will also research emerging threats and relevant current news items will be discussed in class as this will help when applying their knowledge to scenarios in the written examination.
1.3.2 The impact of data loss, theft or manipulation on individuals and businesses	By learning about the impact of data loss, theft or manipulation on individuals and businesses, learners will understand the importance of being vigilant when working

Learners should know and understand the financial, moral and legal implications (including competitor advantage, breaking of GDPR/DPA, open to blackmail). Learners will also gain an understanding about data manipulation, loss of service, intellectual property and reputation.		with data. From a vocational context, the protection of data is fundamental to ensuring good quality data and the success of a business. The financial implication is the difference between success and failure of a company and ensuring they understand this area will help learners make better decisions with the knowledge gained from the previous sections on the importance of data. Learners may be asked to consider the impact of data loss, theft or manipulation on individuals or organisations in the written examination.
1.3.3 Methods used to protect information Learners should know and understand the logical protection of computers including access levels, authentication, firewalls, anti-malware applications, password protection, encryption and physical protection including locks, biometrics, location of hardware, backup systems and security staff. This topic will also explore security policies including disaster recovery, staff responsibilities, acceptable use policy and staff training.		With an understanding of the potential consequences of data loss, learners will appreciate the need to arm themselves with a range of methods with which to protect their information. This will include knowledge of both logical and physical protection methods available, including any new developments. Learners also need to appreciate how companies will have security policies in order to minimise the threat to information stored and this will encourage learners to follow these policies when they start out in the workplace. Standard and common-sense working habits should be adopted in the workplace; for this to happen, learners will be educated about how these measures can be implemented at organisation and individual level. Learners will be encouraged to keep up to date with new protection methods.
1.3.4 How moral and ethical issues affect computer users Learners should know and understand privacy and security, cookies and data collection by multinational companies as well as the monitoring of individuals and impact of data loss or damage.		Learners should understand the moral and ethical issues that affect computer users in order for them to make informed judgements about what is right and wrong. This builds on 1.3.3 where learners must understand the fine line between freedom and responsibility. Learners need to be aware of what cookies are and how they are used to increase brand awareness, whilst considering in what ways their use could affect the more vulnerable population in a negative way. Whilst privacy is protected by a range of measures, learners must understand when a company may want to monitor an individual. Learners will consider the issue from both the side of the individual worker and that of the company managers.

1.3.5 How legal issues protect computer users Learners should know the different legislations and rulings that govern computer use. These laws include General data protection regulation (GDPR) 2018, Data protection act (DPA) 1998, Computer misuse act 1990, Communications act 2003, Regulation of investigatory powers act 2016, Copyright, designs and patents act 1988 and Health and safety legislation.		Learners need to know how legal issues protect computer users so that they understand the parameters and can operate within the law, as well as having an appreciation of how legislation protects their own rights.
1.3.6 The cultural, personal and environmental impact of ICT Learners should be aware of employment patterns including retraining, changes in working practices (e.g., collaboration, hot desking), teleworking and homeworking. Learners will also explore the wider effects of working and working patterns in relation to videoconferencing, effect on transport, effect on traditional media and drones. Learners must also know and be aware of green IT and e-waste in relation to rare earth element mining, global production lines and the digital divide – local and global. Learners will look deeper at social media including cyberbullying and Fake News, net neutrality, addiction and mental health.		The Covid 19 pandemic revealed how working remotely can replace the physical presence in the workplace; with this comes a wide array of tools. From videoconferencing to finding a work-life balance, which may involve a better quality of life due to the lack of commute, learners need to develop an understanding of the pros and cons of homeworking, including the digital divide and access to technology. ICT has an impact on almost every aspect of our lives – from working to socialising, learning to playing. The digital age has transformed the way young people communicate, network, seek help, access information and learn. With environmental issues gaining more and more international attention, learners will appreciate the potential impact of areas such as green IT and non-green IT, e-waste and rare earth element mining. Fake News, cyberbullying and mental health are also hot topics and will be investigated and discussed in the context of ICT impact. Learners will be encouraged to take an interest in the cultural, personal and environmental impact of ICT by discussing news items, documentaries and television programmes
1.3.7 How a digital footprint can impact computer users Learners should know and understand the potential effects of digital footprint – passive and active, posts on social media, online identity, identity theft and the risks of inappropriate images.		Understanding the effects of their digital footprint will help learners choose and control what they leave online for others to find. This knowledge will help learners avoid risks such as identity theft and teach them that leaving a positive digital footprint can be beneficial to their reputation and future opportunities. Through understanding the impact of their digital footprint, learners will be better able to make informed choices about the information they share online. Learners could investigate case studies that

		illustrate how a digital footprint can impact upon people, both positively and negatively. They could also produce their own set of guidelines for creating a positive digital footprint

How can parents help at home?

Parents can help by ensuring revision and homework is completed.

Helpful further reading and discussion

Reading

Level 1/2 Vocational Award ICT Course Companion

https://www.wjec.co.uk/qualifications/level-1-2-vocational-award-in-ict/?sub_nav_level=books#tab_resources