Unit 20: Technological Systems to Support Service Delivery

Delivery guidance

Approaching the unit

In this unit, you will help your learners investigate the information and communication technology (ICT) used by the uniformed protective services, ranging from mobile, handheld devices to evidence captured by drones in missing person cases. Your learners will explore how cyberspace is used by the public, its relationship to cybercrime and its impact on the service and delivery of the protective services.

This is a rapidly changing area and staying up to date is essential. You should try to update your industry experience, and aim to keep updating this within your teaching each year. Your learners will need help researching and understanding the legal and security requirements that the uniformed protective services must follow when using ICT and as with the rest of this unit, this is an area of study that is fast changing so it is important to check the laws every year of teaching.

Inviting guest speakers from local uniformed protective services to talk about the ICT equipment they use, such as a Police Officer talking about Body Worn Cameras and Automatic Number Plate Recognition, the impact it has on their job and the challenges it has created will help bring this unit to life.

For this unit, learners must have access to current information on the different types of ICT used in the uniformed protective services. This is especially important regarding ICT that has been recently introduced. Ideally, understanding how the different types of ICT are used, the skills needed to use them and their benefits could be relayed through visiting active service personnel. For example, learners may be given the opportunity to explore the GCHQ programmes on offer in depth, to fully appreciate how the challenges of cybercrime are being met.

Delivering the Learning Aims

For **Learning aim A** learners should be introduced to the relationship between ICT and the uniformed protective services looking at how it has helped the services share information, work with other services and have better engagement with the communities they serve. Learners should be allowed to research a range of ICT that the uniformed protective services use such as ANPR, BWV, drones, and data systems such as the Police National Computer. After learning about these forms of ICT learners

should look at the advantages and disadvantages of them. To help consider advantages and disadvantages the learners could be introduced to real life case studies of when these ICT systems have worked effectively or poorly.

For **Learning aim B** learners should be allowed to consider what cyberspace is and what challenges it poses to the uniformed protective services. Learners are very aware of cyberspace, and it could be beneficial to allow them to take the lead on any challenges they do not identify. Learners should explore how the UK meets the challenges of cybercrime by researching the agencies involved, such as GCHQ and the National Crime Agency, and the activities they undertake, such as awareness campaigns, to tackle the issues. Learners could design their own awareness campaign to tackle a particular cybercrime. Finally, learners should consider both the positive and negative impact of cybercrime on the uniformed protective services.

For **Learning aim C**, learners need to be introduced to the laws and national and industry standards that govern the uniformed protective services whilst using ICT. Learners must also be aware of a range of security requirements that are needed to keep ICT safe. This could benefit from an ICT expert from the services or an ICT technician from your establishment delivering a presentation to learners to show how this works in real life.

Assessment model

Learning aim	Key content areas	Recommended assessment approach
A Investigate the information and communication technology (ICT) used by the uniformed protective services	**A1** Introduction to ICT in the uniformed protective services **A2** Types of ICT and monitoring equipment	Application to case study on ICT used by a selected uniformed protective service, requiring learners to focus on: • the relationship between ICT and the role in the selected service • the national, regional and local types of ICT used in that service and how effective they are • impact of the technology used within the selected service.
B Explore the impact of cybercrime on the uniformed protective services and how ICT is used to meet challenges	**B1** Challenges presented by cyberspace **B2** Meeting the challenges of cybercrime **B3** Impact on the uniformed protective services	A presentation, with notes, that evaluates the impact of cybercrime on a role in a selected uniformed protective service and how the service meets such challenges. It will include a comparison of the different challenges posed by cyberspace and cybercrime and how they are being met by GCHQ, National Cyber Security Centre, NCA, and the Joint Forces Cyber Group.
C Research the legal and security requirements that the uniformed protective services must follow when using ICT	**C1** Legal requirements **C2** Security requirements **C3** Organisational and individual responsibilities	A report that justifies the legal and security requirements for the uniformed protective services in the use of ICT. The report will focus on: • the different laws that are required when using ICT • the benefits of individual security, and layered cybersecurity • the need to have both legal and security requirements when using ICT.

Assessment guidance

The recommended assessment for this unit includes two assignments. The first assignment focuses on Learning aim A the second on Learning aims B and C. There is a maximum number of two summative assignments for this unit.

For the first assignment you could ask learners to Application to case study on ICT used by a selected uniformed protective service, requiring learners to focus on:
• the relationship between ICT and the role in the selected service
• the national, regional and local types of ICT used in that service and how effective they are
• impact of the technology used within the selected service.

Through the use of a case study the learners are required to describe how a job within a selected protective service is impacted by ICT. The learners must also describe the range of technology used in the selected service. They must examine the short- and long-term impact that the technology has had on a specific uniformed protective service. Learners will also determine the technology's effectiveness in terms of supporting the uniformed protective services, before coming to conclusions about its overall effectiveness.

For assignment 2 learners will pick one uniformed protective service and describe the challenges that cyberspace is causing that service and then explain what the services are doing to deal with these challenges. Learners need to compare the challenges and strategies used by the service leading to an evaluation of how much of a challenge it is to the services and how effectively they are dealing with the challenge using evidence to back up these conclusions. Learners will briefly identify the laws and standards the services must adhere to whilst using ICT and explain the security requirements whilst using ICT in the protective services and its benefits. Learners must then look at the strengths and weaknesses of the legal requirements and security requirements making a justification of why they are required.

Details of links to other BTEC units and qualifications, and to other relevant units/qualifications

This unit links to

- Unit 5: Teamwork, Leadership and Communication in the Uniformed Protective Services
- Unit 7: Planning for and Responding to Emergency Incidents
- Unit 18: Criminal Investigation Procedures and Practice.

Resources

In addition to the resources listed below, publishers are likely to produce Pearson-endorsed textbooks that support this unit of the BTEC Nationals in Uniformed Protective Services. Check the Pearson website (http://qualifications.pearson.com/endorsed-resources) for more information as titles achieve endorsement.

Textbooks

Bryant, R. and Bryant, S., 2016. Policing digital crime. London and New York: Routledge, Taylor & Francis Group.

Ozkaya, E., 2019. Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity. Birmingham; Mumbai: Packt Publishing

Steinberg, J, 2019. Cybersecurity for Dummies. Hoboken, NJ: John Wiley & Sons Inc.

Journals
Fire
Police Review
Soldier Magazine

Websites

https://www.gchq.gov.uk/section/mission/cyber-security

https://www.ncsc.gov.uk/

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

https://www.met.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/

https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime