THE PARK ACADEMIES TRUST SIXTH FORM
Don't be anonymous...
...be remarkable

Cyber Security & Networks

Level 3 Cambridge Advanced National in Cyber Security and Networks is a Alternative Academic Qualification equivalent to 1 A Level. This builds upon the IT skills students developed at KS4.

The course has been developed to meet the challenging needs of the IT sector and prepare students for Higher Education or employment.

The course supports the transferable skills required by universities and employers such as critical thinking, problem solving, time management, independent learning and research skills.

Extended Certificate

56 UCAS points available

Student Profile

A successful student will:

Have achieved a Level 2 Merit in the CNAT IT or Creative iMedia courses or band 4 in GCSE Computer Science or an equivalent IT KS4 qualification.

Be interested in developing the knowledge and skills you need to be a competent and informed IT user and practitioner.

Seek to develop their knowledge of Cyber Security and Networks to ensure computer systems are set up safely and securely.

Be interested in a career using technology.

The Park Academies Trust

Course Content (Cambridge OCR)

This qualification is assessed through a combination of 2 written examinations and 3 coursework units totalling 360 guided learning hours (GLH).

Unit F193 - Fundamentals of Cyber Security (75 GLH Exam): this unit will cover why Cyber Security is important to us all and the motivations of different threat actors, how threats function and steps to take to protect, detect and respond to them.

Unit F194 - Fundamentals of Networks (70 GLH Exam): this unit will look at fundamental concepts of networks including different models, hardware and protocols.

Unit F195 - Preventing Cyberattacks (75 GLH Coursework): this unit will teach the techniques to assess for risks to networks, devices and applications and how to design policies and control access to systems and how to educate users in cyberattack prevention.

Unit F196 - Digital Forensic Investigation (70 GLH Coursework): this unit looks at the digital forensic processes followed when completing investigations. You will use software tools to extract evidence and know how to prepare it for its use in court proceedings.

Unit F197 - Penetration Testing and Incidence Response (70 GLH Coursework): this unit will focus on penetration testing strategies. Students will learn how to create cyber security incident response plans, incident playbooks and maintenance plans.

Skills Gained

This qualification enables students to get hands on with the practical elements of cyber security and networks.

Students will be able to apply their knowledge to practical, real lift contexts such as assessing the risks to networks, devices and applications and creating risk assessments. Auditing measures used to prevent cyberattacks and planning digital forensic investigations.

Furthermore students will learn how to plan, scope, design and secure computer systems to meet client and user requirements.

Trips/Cultural Experiences

Bletchley Park, Milton Keynes - home of the World War Two Codebreakers

Museum of Computing - Swindon

The Future - What Next?

Successful completion could lead to a degree in related subjects such as Cyber Security, Network Engineering, Ethical Hacking, Digital Forensics or Computer Science. The skills developed could also lead into IT Technical Support, Cyber Security and Network Maintenance related careers.

Helen Plumb

BSc (Hons) Combined Studies in Sciences, MSc Evolutionary & Adaptive Systems, PGCE

Teacher of Computing, Cyber Security & Networks / Data Manager & Timetable Manager

PlumbH@
lydiardparkacademy.org.uk

Will Day

BSc (Hons) Cyber Security Management, PGCE

Teacher of Computer Science, Cyber Security & Networks / Online Safety Officer

DayW@
lydiardparkacademy.org.uk