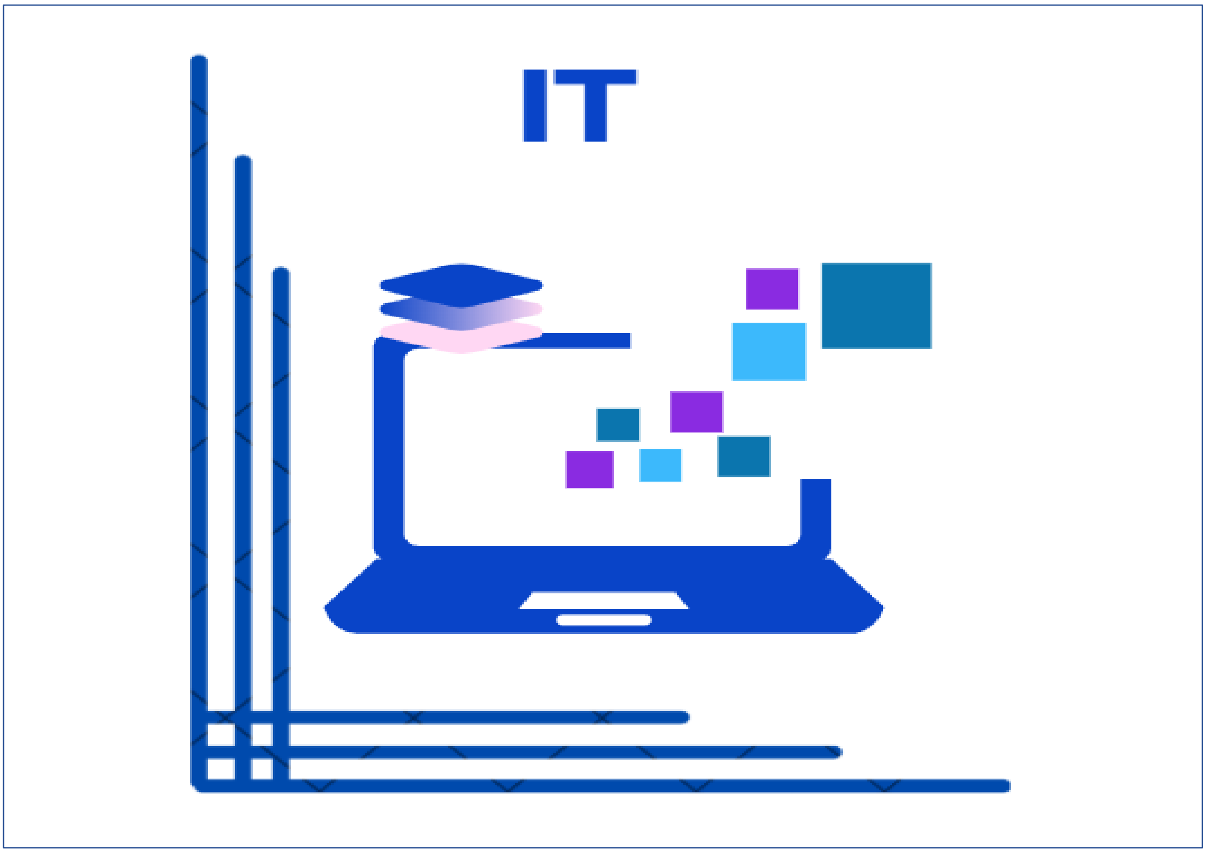
Year 11 > 12 Bridging Work
Summer Term 2025



Subject	IT
Course	Level 3 National Extended Certificate in Information Technology (AAQ)
Awarding Body	Pearson BTEC

Contents:

Course/specification overview

The Pearson BTEC Level 3 National Extended Certificate in Information Technology (AAQ) allows students to study the fundamental knowledge of Information Technology covering the role and implications of using Information Technology systems and cyber-security threats and how to manage attacks. Students will also develop important skills for creating websites to meet a specific purpose and to manage data through the development of a relational database solution.

There are two examined units and two internally assessed units where students will engage in practical tasks to develop their Information Technology skills and knowledge.

The qualification is designed to be taken alongside A levels as part of a study programme and can link to learning in A level Mathematics and A level Business Studies. It is intended for students that wish to progress into higher education as a pathway to employment.

What will you study as part of this qualification?

The qualification has been developed in consultation with higher education representatives and sector experts to ensure students have the knowledge, understanding and skills they need to progress to, and thrive, in higher education.

Students must complete four mandatory units.

Unit Number	Unit Title	GLH	Type	How it's assessed
1	Information Technology Systems	120	**Mandatory**	External
2	Cyber Security and Incident Management	120	**Mandatory**	External
3	Website Development	60	**Mandatory**	Internal
4	Relational Database Development	60	**Mandatory**	Internal

1. **Information Technology Systems** – Information technology systems, including the relationship between software and hardware, and the issues related to IT systems

2. **Cyber Security and Incident Management -** Types of cyber security attacks, the vulnerabilities in networked systems and how to plan and respond to attacks

3. **Website Development** – The development tools, techniques and processes used in website development and how to test usability, functionality and fitness for purpose

4. **Relational Database Development** – Structure of data, data design and database management systems (DBMS)

External assessment

66.6% of the total qualification GLH is made up of external assessment. A summary is given below.

Unit	Type	Availability
Unit 1: Information Technology Systems	• An external examination set and marked by Pearson • 90 marks	**January and June First assessment June 2026**
Unit 2: Cyber Security and Incident Management	• An external examination set and marked by Pearson • 90 marks	**January and June First assessment June 2026**

For further information the course specification can be found here.

Our Department expectations

Expectations

The ICT department has high expectations of students. We expect you to be engaged and willing to learn for yourself, be respectful to others in your classes and make your very best efforts in all lessons and homework. All homework and coursework is to be submitted by the deadline stated and in the required format. In return your teachers will provide you with regular feedback to enable you to progress.

Lesson Preparation and Organisation

- Pre-reading from textbook or online when requested.
- Regularly check your email and Satchel One.

Independent Study

•Catch up on missed work due to absences

•Use non-contact study periods (timetabled) for pre-reading, structured reviewing of learned material and practical work as required

•Revision for end of unit tests and exams

•Use study skills and revision skills that have been taught to you

•If below target grade, must attend coursework catch up sessions to make sure coursework is up to standard.

Review/revise

The foundations of key skills, knowledge and understanding which should be secure from GCSE or interdisciplinary learning in related subjects, where the subject may be new to Learners of Post-16 are transferable skills these are:

- The ability to learn independently.
- The ability to research actively and methodically.
- To be able to give presentations and be active group members.
- Cognitive and problem-solving skills: use critical thinking, approach non-routine problems applying expert and creative solutions, use systems and technology.
- Intrapersonal skills: communicating, working collaboratively, negotiating and influencing, self-presentation.
- Interpersonal skills: self-management, adaptability and resilience, self-monitoring and development.

Learners can also benefit from opportunities for deep learning where they are able to make connections among units and select areas of interest for detailed study. These skills required for particular degree courses, including:

- Reading technical texts
- Effective writing
- Analytical skills
- Creative development
- Preparation for assessment methods used in degrees.

Watch

To prepare for the course Learners can watch and visit these suggested websites, which support in the understanding of certain topics in the course.

- Physical Security video series:

https://www.youtube.com/watch?v=s6QsNOj4URA

- Dynamic Host Configuration Protocol (DHCP)

https://www.youtube.com/watch?v=IdtUSSZJCGg

- A cyber security policy that uses the Plan-Do Check-Act

https://www.youtube.com/watch?v=n6BW3Tv1vAw

- Business continuity and disaster recovery planning?

https://www.youtube.com/watch?v=o0xj1JKjjOE

- How to use Wireshark

https://www.youtube.com/watch?v=zWoHJ3oGRGY

- How to review network logs with event viewer

https://www.youtube.com/watch?v=PO2g5oYDpJQ

Listen to

- **TWiT**
  TWiT is a popular general tech podcast, while "Heavy Networking," "Cloudcast," and "Risky Business" delve into specific areas like networking, cloud computing, and cybersecurity, respectively.
  https://twit.tv/

- **The MKBHD Podcast:**
  The MKBHD (Marques Brownlee) Podcast provides in-depth reviews and analysis of technology, including smartphones, gadgets, and software.
  https://www.youtube.com/user/marquesbrownlee

Read

- Laudon, K. C. & Laudon, J. P., Management Information Systems: ***"Managing the Digital Firm"***, Pearson, 2018 (ISBN 978-0-13-480157-0)

- O'Brien, J. A. & Marakas, G. M., **"Management Information Systems"**, McGraw-Hill Education, 2016 (ISBN 978-0-07-337683-1)

- Rainer, R. K. & Turban, E., Introduction to Information Systems: ***"Supporting and Transforming Business"***, Wiley, 2018 (ISBN 978-1-118-03868-0)

- Shelly, G. B. & Vermaat, M. E., Discovering Computers: ***"Digital Technology, Data, and Devices",*** Cengage Learning, 2018 (ISBN 978-1-305-25800-0)

- Stair, R. & Reynolds, G. W., ***"Principles of Information Systems"***, Cengage Learning, 2017 (ISBN 978-1-305-24845-2)

Research

In order to start the course, learners can research suggested activities prior to starting the course:

Activity 1:

Research Projects: Learners to research a current technological challenge e.g., AI Ethics or Data Privacy Issues and prepare a presentation or report. This activity will encourage learners to gather evidence, analyse data, and articulate their findings clearly. This activity could be word processed or presented as a PowerPoint.

Activity 2:

Technology Impact Analysis: Learners choose a specific technology e.g., Social Media or Cloud computing and analyse its positive and negative impacts on society. This activity will promote critical evaluation of technology's role in modern life. This activity could be word processed or presented as a PowerPoint.

Complete

Learners can complete the suggested pre-course activities:

Activity 1:

The National Cyber Security Centre (NCSC) role is protecting UK organisations, public services, and individuals from cyber threats. The NCSC provides resources, updates, and guidance to improve national cyber resilience.
The importance of foundational cyber security knowledge for all staff and how the NCSC training can build awareness and practical skills.
The NCSC Cyber Security Training offer staff training and staff website introduces the key topics it covers, such as passwords, phishing, and device security. The objectives of the training, which are to understand basic cyber security practices and recognise common security threats in professional settings.
Complete the training independently, taking notes on key practices and tips that you have learnt e.g.:

- Key tips for securing information and devices.
- Methods to identify phishing attempts and suspicious communications.
- Strategies for creating and managing strong passwords.
- Reflect on how these principles apply not only to organisational settings but also to personal cyber security.

The training can be found at:
https://www.ncsc.gov.uk/training/v4/Top+tips/Web+package/content/index.html#/
Use Ms Word to produce your findings.

Activity 2:

In this activity you will look at emerging technologies, we will look at , AI, Blockchain Technology and Virtual Reality

***TechCrunch.com* -** provides the latest news on emerging technologies, start-ups, and trends in the tech industry.

Discuss the potential benefits and challenges associated with these technologies, focusing on its implications for personal use and organisational performance.

Select a case study from "*https://www.ibm.com/watson*" which is a website that provides resources and case studies on artificial intelligence and other emerging technologies and study of an organisation that successfully implemented an emerging technology to improve IT systems performance.

Write a reflective essay on the implications of this technology on the organisation's operations. Use Ms Word to produce your findings.