MET Brighton
Metropolitan
College

Digital Industries

Level 3 T Level | Digital Support Services & Security|

Course details

Course code: MITP010

Campus: Brighton – Central

Attendance: Full Time

Duration: 2 Years

Qualification: T Level in Digital Support Services & Security| Level 3

Dear Student,

We're delighted to welcome you to Brighton MET College and are very much looking forward to you joining us this September.

During your first week, you'll receive key information about the course, the department, and the college. This will include your timetable and course handbook. Your tutor will introduce you to the structure of the course and assessments, outline the exciting work-related experiences you'll take part in, and explain our expectations of you as a student at Brighton MET.

We can't wait to support you on this creative and professional journey.

Best wishes,

Karena Morrison

Teaching & Learning Manager

What to bring on your first day

- ✓ A pen and/or pencil and a notebook
- ✓ Water bottle
- ✓ Work from Summer Project

Summer Project

Your Mobile, Your Data – A Security Audit

Project Aim:

This summer you'll investigate just how secure your mobile device really is – and how much of your personal (and passive) data is being harvested. By the end, you'll have carried out a full **security audit** of your phone, evaluated current **mobile threats**, and reflected on how you protect yourself (or don't!).

What You'll Be Doing:

You'll carry out an audit and complete a short report or presentation. Your project should cover the following **technical areas**:

Security Audit – Your Device

Carry out a full technical audit of your device. You should **record your findings**, include screenshots where possible, and explain what they mean. Key areas to check:

1. Lock screen settings (PIN, biometrics, timeout)
2. Encryption status (enabled or not)
3. OS version (up to date?)
4. Installed antivirus/security apps (name, purpose)
5. App permission list (what apps are accessing location, camera, mic, SMS, etc.)
6. Accessibility permissions (can any app control your phone?)
7. App store settings (can unknown apps be installed?)
8. Any rooted/jailbroken modifications?

Tip: Use your phone's **Settings > Privacy** and **Security** sections.

Data Collection – What Are You Sharing?

Use your **Google account (or Apple ID)** to find out:

1. What search history, voice commands, YouTube views, app usage and location data is being collected
2. What permissions are granted to third-party apps (linked accounts, access tokens, etc.)

3. Run a **Google Privacy Check-up** and/or download your data via **Google Takeout** - [How to download your Google data - Google Account Help](#)
4. Reflect: How much data surprised you? Did you know this was being collected?

Mobile Security Threats – Investigate

Research and summarise **at least 4 of the top mobile security threats**. You can use the list below or choose your own. For each, describe:

1. What is it?
2. How does it work?
3. What could it do to your device or data?
4. How could it be prevented or mitigated?

Example Threats to Choose From:

1. Malicious apps (banking malware, adware, etc.)
2. Spyware & stalkerware
3. Ransomware
4. Mobile phishing / smishing
5. Device hijacking (SIM swap)
6. Man-in-the-middle attacks (unsecured WiFi)
7. Weak passwords and brute force
8. Rooting/jailbreaking vulnerabilities
9. Lost/stolen device access
10. OS/firmware exploits

Risk Reflection: What Are You Doing About It?

Once you've identified risks and checked your own phone:

1. What have you **already done** to protect yourself?
2. What **risks have you ignored or underestimated**?
3. What changes have you made since starting this project?
4. Are your family or friends aware of these risks? What would you advise them?

Stretch Task (Optional):

Choose **one real-world case study** (e.g. the Pegasus spyware attack, SIM-swap fraud, or a high-profile phone hack) and explain:

1. What happened?
2. What vulnerability was exploited?

3. How could it have been prevented?

What to Hand In (Formats):

You can present this as:

1. A PowerPoint presentation (with screenshots)
2. A written report or case study (Word or PDF)
3. A short video walkthrough explaining your audit (screen recording + commentary)
4. An infographic summarising key findings

Include:

1. A title
2. Your name
3. Screenshots/photos where possible
4. Your reflections at the end

Deadline:

Bring your finished project with you for enrolment or induction week in September. Be prepared to talk about what you found surprising, and what you changed on your device!

Why This Matters (Work Readiness):

Digital support professionals need to:

1. Understand device-level security
2. Communicate risks clearly to users
3. Recognise and mitigate threats
4. Support ethical and legal data handling (e.g. GDPR)
5. Think critically about technology use
6. This project gives you a **head start in all of these areas**.

Submission:

- **Deadline**: 02nd of August 2025
- **Method**: Submit your completed project via email.

Support:

If you have any questions or are unsure how to complete this task please get in touch.

We look forward to seeing your reflections and plans. Have a great summer, and we can't wait to start this journey with you in September.

Financial support

Information can be found on our main website: brightonmet.ac.uk

Go to 'help and support' then 'financial support'

CLICK TO VIEW

Link to LSG (Learner Support Grant) application
CLICK TO VIEW

OTHER INFO

You will be taking part in enrichment trips and activities during the academic year. One of these trips is a visit to Bletchley Park. All students are expected to contribute a one-off payment of £50 towards these trips. You will be invoiced nearer the time of the trip.

Contact details:

Stephen Robinson
T-Level (Digital Support Services) Course Lead
WBL Apprenticeship Assessor
Brighton MET College
Email: stephen.robinson@gbmc.ac.uk
Brighton Met: 01273 667788 Extn 2256

Or

Support office:
Games.computing@gbmc.ac.uk