1.1 Question 1: Incidents and Incident Response

Reaction Situations Summary:

Higher education's continued reliance on digital platforms for assessment submission and evaluation makes it more crucial than ever to take security risks into consideration. Here, we look at a real-world academic workflow: a postgraduate student must use a cloud storage service like Dropbox or Google Drive to turn in the source code for their entire software project. Academic staff can access the file remotely for auditing and decision-making purposes. An issue arises, though, when the submission folder or link is set up in a way that permits unauthorised access or even alteration by outside parties. Through impersonation, exploitation of lax access controls, or intercepting the shared link, an attacker could obtain access to the cloud folder. There could be repercussions for both academic and security purposes if they change the source code, replace it with content that has been plagiarised, add malicious payloads, or corrupt files. The scenario highlights several forensic readiness concerns, including protecting digital evidence, upholding authenticity and integrity, and stopping wrongdoing like text misattribution, collusion, impersonation, and generative AI abuse.

Risk Scenario Discussion:

The primary risk in this case is that the original submission might be altered or changed covertly before the marker has a chance to view it. There are concerns regarding file integrity, submitter authenticity, and the capacity to carry out a suitable forensic investigation in the event of a dispute because the submission was made via a cloud service that the institution does not fully control.

This allows for a variety of wrongdoings:

- Collusion or Misattribution: When a student turns in work that contains code from an online source or another student without giving credit, this is known as misattribution.
- Subcontracting or impersonation: A third party, or even a for-profit company, may submit or alter the project on the student's behalf.
- GenAI use that goes unreported: Text or code produced by AI tools may be submitted as original work with no explanation.
- Tampering: When a file is submitted, a malevolent third party alters it, possibly to introduce vulnerabilities or tamper with another student's grade. Setting Off Investigational Events:
- Unusual code is similarly flagged by a plagiarism detection tool.
- The metadata for the file does not correspond to the anticipated submission time.
- When a file is altered, the student disputes who wrote it or who owns it.

- The marker observes discrepancies between the student's known abilities and the code structure.
- Unauthorised access or data leaks are reported by outside parties.
- The student who turned in the assignment is one of the interested parties.
- The instructor or grader in charge of evaluation.
- The moderator or second setter confirming the marking procedure. •Academic fairness is audited by the external examiner.
- The legal and IT departments of the university.
- Students whose work may have been altered or plagiarised. Probability, Severity, and Possible Loss Event:
- Loss Event: Assignment misattribution, unauthorised access, or integrity violation.
- Probability: Moderate to high, contingent upon student awareness and the university's secure submission policy.
- Severity: Appeals, high-risk student failure, harm to the institution's reputation, and unethical behaviour.

Forensic Readiness Measures:

The proactive setup of procedures, systems, and policies to facilitate efficient digital investigations in the event of a security breach or academic misconduct is known as 'forensic readiness'. The recommended actions listed below are divided into three groups: long-term institutional measures (following the incident), incident management (during the incident), and anticipatory (prior to the incident).

Anticipatory Measures (Before the Incident):

- Use of Safe, Institution-Controlled Submission Systems: The only way to submit should be through university-owned portals like Moodle or Blackboard. Reliance on public cloud platforms should be avoided unless access controls are clearly specified.
- Cryptographic Hash Submission: Prior to the due date, students must create and turn in SHA-256 hashes of their project files. This enables file integrity to be checked later.
- Digital Signatures and Timestamping: Submissions ought to be timestamped by a reliable authority and signed with public-private key encryption. This makes it possible to verify the file's origin and time.
- Multi-factor authentication (MFA) for submission access: To lower the risk of unauthorised access, staff and students using cloud storage or submission platforms must employ MFA.
- Academic integrity declarations: A signed digital declaration attesting to the work's originality, disclosing any use of artificial intelligence, and confirming that no unapproved collaboration took place should be included with every submission.
- Brief video presentations: To show ownership and authorship, students can choose to record a brief video describing their project.
  In any dispute, this could be used as proof.

Measures for Incident Management (During and Right After):

- Evidence preservation: Cloud storage and any pertinent metadata, such as IP addresses, timestamps, and access logs, must be forensically preserved as soon as a problem is suspected. It is necessary to create a write-protected copy of the original file.
- Hash Verification: Compare the student-submitted hash with the staff-retrieved submission hash. Unauthorised changes would be indicated by a mismatch.
- Access log review: To determine who accessed the file, when, and from which IP address, investigators must examine access logs. Basic log history is provided by services like Dropbox, OneDrive, and Google Drive.
- Chain of custody documentation: To ensure admissibility in academic proceedings, all gathered evidence must adhere to stringent documentation guidelines.
- Student interview: To determine authorship, conduct an academic interview with the student to see if they can effectively defend and explain their work.
- If required, involve the academic misconduct panel: Take the matter to a formal review once enough proof has been gathered. Make sure that any decision is supported by documented forensic procedures.

Long-Term Response measures (Post-Incident Improvements):

- Policy Updates: The use of AI tools, submissions to third-party clouds, and ownership of digital work should all be specifically covered by institutional policies.
- Using secure portals is required: Block links to cloud-sharing resources for coursework. Provide MFA access and audit trails for institutional platforms.
- Consistent training for staff and students: Implement seminars on detecting academic misconduct, digital evidence, and the moral application of technology, including GenAI.
- Integration of cloud forensics: Collaborate with cloud providers who offer immutability (such as version history), forensic logging, and compliance with the UK GDPR and CMA.
- Regular audits of forensic preparedness: Conduct yearly or semi-annual evaluations of evidence handling procedures, forensic tools, and submission practices.

Resolution Pathways:

- In the event of a disagreement:
    - A forensic report is shown to the academic panel.
    - The student is given an opportunity to reply.
    - Authenticity is evaluated using evidence such as hashes, timestamps, and interviews.
    - If the decision is appealed, an external examiner may review it.

1.2 Question 2: Legislation and Regulations – Alice and Bob Case

Scenario Recap:

Alice is a CStGUoL student. Her friend Bob, who attends Middlesex University, requests permission to use Alice's work laptop to submit his own coursework using the inline submission system at his university. He is permitted to use an open tab in his browser by Alice. Which UK laws apply, under what conditions, and whether this behaviour could be considered a criminal offence are the questions at hand.

Is this a criminal offence?

Probably yes – depending on the device and access authorisation.
If Alice's laptop is personally owned, and Bob simply uses it to submit his own work to his own university, there is no offence.
However, if Alice's laptop is owned or managed by the university (CStGUoL) and:

- She is not permitted to allow others to use it.
- Bob's access violates the university's Acceptable Use Policy.
- And/or Bob is using it for purposes unrelated to the university's business.

Then this may constitute unauthorised access under Section 1 of the UK Computer Misuse Act 1990.

Legal Reference:

- Computer Misuse Act 1990, Section 1:

"A person is guilty of an offence if—
(a) they cause a computer to perform any function with intent to secure access to any program or data,
(b) the access intended is unauthorised, and
(c) They know at the time that this is the case."
(Legislation Link)

Who is the offender (if any):

- Bob is the likely offender if access to Alice's device was not authorised by the university.
- Alice may be indirectly at fault if she knowingly allowed unauthorised use of institutional property, but she would more likely be held accountable through internal disciplinary procedures rather than criminal liability.

1.2.1 – Sub-question 2a: Academic and Legal Literature

To deepen the analysis, we turn to at least three academic and industry sources that discuss legal, ethical, and technological perspectives on unauthorised access.

- Vacca (2020) – Computer and Information Security Handbook

Vacca discusses how institutional policy sets the boundary for authorised access. If a student permits someone to access a device they are not permitted to share, this access may breach security principles and legal boundaries.
"Authorised use must be granted by the system's true owner—not merely the user in possession of the device."

- Tavani (2016) – Ethics and Technology
  Tavani explores the ethics of access in computing environments, highlighting that consent by an individual does not necessarily imply lawful access.
  "Authorisation must be consistent with both organisational policy and legal structures."
- Coles-Kemp and Overill (2007) – Insider Threats in Security
  The authors discuss how "friendly" or unintended insiders—such as friends borrowing devices—can introduce significant policy and legal risks, often without malicious intent.
  "Unintentional insider access remains one of the hardest threats to mitigate."

In conclusion

In academic settings, it can be difficult to distinguish between digital misconduct and ethical favour. Digital forensics, institutional policy, and UK law play a crucial role in establishing accountability, handling incidents, and maintaining trust in both cases.

References:

1. National Institute of Standards and Technology (NIST), 2006. *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)*. [online] Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf [Accessed 15 April 2025].
2. Computer Misuse Act 1990. *UK Public General Acts: Chapter 18*. [online] Available at: https://www.legislation.gov.uk/ukpga/1990/18/section/1 [Accessed 12 April 2025].
3. Vacca, J.R., 2020. *Computer and Information Security Handbook*. 4th ed. Cambridge, MA: Academic Press.
4. Tavani, H.T., 2016. *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing*. 5th ed. Hoboken, NJ: Wiley.
5. Coles-Kemp, L. and Overill, R.E., 2007. Insider threats in security: A framework for analysis. In: *Proceedings of the 2007 International Conference on Cyberworlds*. Washington, DC: IEEE Computer Society, pp. 83–87.