Functional Skills English Level 1

Mock Test 5

Total marks: 57

Pass mark: 34 out of 57

Time allowed: 2 hours

Reading 21 marks | Writing 36 marks | Time: 2 hours. Spend roughly 45 minutes on reading and 75 minutes on writing.

You will need: pen, pencil, ruler, rubber. Dictionary allowed for Reading section.

Name: _____ Date: _____

Text 1: Article from a community newspaper

Scam Alert: Why We All Need to Think Before We Click

Online fraud cost UK consumers £2.3 billion last year, according to figures released by Action Fraud. From fake delivery messages to phishing emails that look like they come from your bank, criminals are becoming increasingly sophisticated in their methods.

One of the fastest-growing scams involves text messages claiming a parcel could not be delivered and asking you to click a link to reschedule. The link leads to a convincing but fake website that asks for your name, address, and bank details. Last year alone, over 45,000 people reported losing money through parcel delivery scams.

"These messages are designed to create panic," explains Sarah Jennings, a cybersecurity advisor at the National Cyber Security Centre. "They arrive when you're busy, and they rely on you acting quickly without stopping to think. That split second of doubt is your best defence."

Older adults are often assumed to be the main targets, but recent data tells a different story. People aged 25-34 actually reported the highest number of fraud cases, largely because they do more of their shopping, banking, and socialising online.

The warning signs are often hiding in plain sight: misspelled sender names, urgent language demanding immediate action, links that don't match the company's real website, and requests for personal information that a genuine company would never ask for by text or email.

Experts recommend a simple rule: if a message asks you to click a link or share personal details, go directly to the company's official website or call them using the number on their website — never use the contact details provided in the suspicious message itself.

Text 2: Workplace Policy Document

Greenfield Logistics Ltd — Social Media Policy for Employees

1. Purpose: This policy sets out the company's expectations regarding employees' use of social media, both during working hours and in their personal time where it may affect the company's reputation.

2. Scope: This policy applies to all employees, contractors, and agency workers engaged by Greenfield Logistics Ltd. "Social media" includes but is not limited to Facebook, Instagram, X (formerly Twitter), TikTok, LinkedIn, YouTube, blogs, and online forums.

3. Personal use during work hours: Limited personal use of social media during breaks is permitted. Accessing social media during working hours for non-work purposes is not allowed and may result in disciplinary action.

4. Representing the company: Employees must not post content that could reasonably be seen as representing the views of Greenfield Logistics unless specifically authorised by the Communications Manager. Any official company social media activity must be approved in advance.

5. Confidential information: Employees must never share confidential business information, client details, financial data, or internal documents on social media. This obligation continues after employment ends.

6. Conduct: Employees must not post content that is discriminatory, harassing, threatening, or defamatory towards colleagues, clients, or the company. Content that brings the company into disrepute, even if posted outside working hours, may be treated as a disciplinary matter.

7. Breach of policy: Any breach of this policy may result in disciplinary action up to and including dismissal. Serious breaches, such as sharing confidential client data, will be referred to the company's legal team and may result in legal proceedings.

8. Reporting concerns: If you become aware of any social media activity that may breach this policy, report it to your line manager or the HR department. Reports will be treated confidentially.

Section A — Reading

11 questions • 21 marks

Question 1 (1 mark)

How much did online fraud cost UK consumers last year?

- A) £2.3 billion
- B) £1.2 billion
- C) £3.5 billion
- D) £4.5 billion

Question 2 (1 mark)

Which age group reported the highest number of fraud cases?

- A) 25-34
- B) Under 18
- C) 45-54
- D) Over 65

Question 3 (2 marks)

Sarah Jennings says scam messages "rely on you acting quickly without stopping to think." What does this suggest about how scammers operate?

- A) Scammers deliberately create urgency and pressure because people are less likely to spot problems when they rush. They exploit busy moments when victims don't have time to check details carefully.
- B) Scammers only send messages at night
- C) They target people who never use the internet
- D) They only send messages to elderly people

Question 4 (2 marks)

The article says older adults "are often assumed to be the main targets." How does the article challenge this assumption?

- A) It provides data showing 25-34 year olds report the most fraud cases, and explains this is because younger people do more activity online — directly contradicting the stereotype
- B) It says older adults never get scammed
- C) It ignores older adults completely
- D) It says younger people are more gullible

Question 5 (2 marks)

Name FOUR warning signs of a scam message listed in the article.

- A) Misspelled sender names, urgent language demanding immediate action, links that don't match the real website, and requests for personal information
- B) Poor grammar, sent at midnight, very long message, and no images
- C) Written in capitals, sent from abroad, asks for your age, and contains photos
- D) Coloured text, multiple attachments, foreign language, and no subject line

Question 6 (1 mark)

When are employees allowed to use social media for personal purposes?

- A) During breaks only
- B) At any time during the working day
- C) Only at weekends
- D) Never — it is completely banned

Question 7 (2 marks)

The policy says the confidentiality obligation "continues after employment ends." Why do you think this clause is included?

- A) To prevent former employees from sharing sensitive company or client information after they leave, which could damage the business or breach data protection
- B) To stop employees from getting new jobs
- C) Because former employees can still access company computers
- D) To ensure employees stay friends with colleagues after leaving

Question 8 (2 marks)

Marcus works for Greenfield Logistics and posts a joke on his personal Facebook account making fun of a client. He argues this is his private life and the company cannot punish him. Is he correct? Explain using the policy.

- A) No. Section 6 states that content bringing the company into disrepute, even if posted outside working hours, may be treated as a disciplinary matter. Mocking a client could damage the company's reputation.
- B) Yes — the policy only covers posts made during work hours
- C) Yes — Facebook is a private platform so the company has no say
- D) No, but only because he used his real name

Question 9 (2 marks)

What is the most serious consequence of breaching the social media policy? Give an example of a breach that could lead to this.

- A) Legal proceedings. Example: sharing confidential client data on social media, which could breach data protection laws.
- B) A verbal warning for checking Instagram at lunch
- C) Having your social media account deleted
- D) Being moved to a different department

Question 10 (3 marks)

Compare the purpose, audience, and language of Text 1 and Text 2. How does each text suit its intended audience?

- A) Text 1 is a newspaper article aimed at the general public using accessible, informative language with statistics and expert quotes to raise awareness. Text 2 is a workplace policy aimed at employees using formal, directive language with numbered sections and clear consequences.
- B) Both texts are aimed at the same audience and use the same style
- C) Text 1 is more formal and rule-based than Text 2
- D) Text 2 is designed to entertain readers like Text 1

Question 11 (3 marks)

Both texts deal with risks connected to using the internet. How does each text approach the idea of protecting yourself online? Which do you find more useful, and why?

- A) Text 1 gives personal safety advice using real-world examples (parcel scams, warning signs) relevant to everyone. Text 2 sets formal workplace rules about responsible online conduct backed by consequences. Text 1 is more broadly useful for everyday life; Text 2 is essential in a work context.
- B) Only Text 1 is about online safety; Text 2 is about office rules
- C) Text 2 is more useful because it has punishments
- D) Neither text gives any useful advice about online safety

Section B — Writing

Complete both writing tasks.

Task 1 — Formal Report with Recommendations (21 marks)

Your workplace has had several staff members fall victim to online scams. Your manager has asked you to write a formal report recommending how the company could improve staff awareness of online fraud.

In your report you should: explain why online fraud is a growing problem (use evidence from Text 1); describe the risks to the company and its employees; recommend at least two practical steps the company could take; use a clear, professional structure with a heading and subheadings.

Write 150–200 words. Use formal language.

Marking: Content & purpose (7) | Organisation & format (7) | SPaG (7)

Task 2 — Informal Message to a Friend or Family Member (15 marks)

Write a message to a friend or family member who you think may not be aware of online scam risks. Warn them about common scams and give them practical advice to stay safe.

In your message you should: explain why you are writing to them; describe at least one common scam (you can use information from Text 1); give clear, practical advice on how to stay safe.

Write 100–150 words. Use an informal but clear tone.

Marking: Content & purpose (5) | Organisation (5) | SPaG (5)