General Certificate of Education
June 2010
Advanced Level Examination

Information and Communication Technology INFO3/PM

Unit 3 The Use of ICT in the Digital World

Candidate Booklet for the June 2010 examination

To be given to candidates on or after 15 March 2010

Information and Guidance

1 On receipt of this booklet, you are advised to check carefully that it is complete and that no pages are missing or illegible. There should be eight pages. If there are any problems you should consult your teacher.

2 The material contained in this booklet is provided for you to use in preparing for Section A of the INFO3 examination.

3 Prior to the examination, your teacher may give you assistance and advice to help you understand the content of this material.

4 You should use the time between receiving this material and the examination to familiarise yourself with its contents.

5 You are allowed to make comments or annotations on this copy of the material but you are **not** allowed to take this copy, or any other materials, into the examination.

6 A clean copy of this booklet will be provided in the examination with the INFO3 question paper, so there is no benefit from learning the contents by rote.

7 The INFO3 examination is on **Monday 14 June 2010** (afternoon session).

Globemob International PLC

Minutes of a Board Meeting to discuss ICT issues.
March 1, 2010

PRESENT:	Chief Executive Officer	Ms J Evans
	Sales Director	Mr M O'Connor
	Finance Director	Mr L Cheng
	ICT Director	Ms C Broussard
	Company Secretary	Mr J Smith
	Human Resources Director	Mrs I Gupta

1. The minutes of the meeting held on February 1, 2010 were accepted as a true record.

2. Ms Evans explained that she had engaged the services of external consultants to advise regarding future ICT activity. The following observations and recommendations, received previously, were discussed:

2.1 Failed ICT Projects.
The consultants had considered previous ICT projects that had failed to deliver the anticipated benefits to the business. They had suggested these failures could have been avoided if there had been sufficient involvement by management and end users in the development of the solutions. Those present accepted this observation.

2.2 ICT Strategy.
Those present accepted the consultants' recommendation that Globemob's ICT strategy needed revision in order to provide better support for the business strategy. Ms Evans pointed out the consultants' advice that Globemob should take into account emerging technologies when formulating a new ICT strategy.

It was agreed that Mr Smith would chair a sub-committee consisting of Mr O'Connor, Ms Broussard and Mr Cheng to discuss ICT strategy and to prepare a draft ICT strategy document for the Board to consider at its next meeting.

Action: JS/MO/CB/LC

2.3 External ICT services.
One of the consultants' recommendations was that external providers be used for all ICT services, including the use of outsourcing. Mr Cheng agreed with this suggestion but Ms Broussard argued that using external services would cause problems.

Ms Evans suggested that Ms Broussard put her concerns in writing for consideration at the next Board meeting.

Action: CB

Turn over ▸

2.4 Information Security Policy.
The consultants had considered the current Information Security Policy (attached to these minutes) to be inadequate for current and future operations and had quoted a cost of £23,000 for it to be brought up to date.

Those present agreed that they needed to understand why the Information Security Policy required updating and Ms Evans agreed to ask the consultants to provide further information.

Action: JE

3. Those present were reminded of the confidential nature of the discussions.

4. There being no other business, the next meeting was scheduled for April 6, 2010.

GLOBEMOB INTERNATIONAL PLC

INFORMATION SECURITY POLICY

1 INTRODUCTION

1.1 The purpose of this information security policy is to meet legislative requirements and to safeguard the Company from accidental or deliberate misuse of computer systems.

1.2 The guiding principles for information security are described, followed by the measures to be adopted by all staff. The Company recognises that the information revolution has fundamentally changed the way we communicate and store information for both professional and personal use; this policy specifically addresses the issues involved and provides guidance.

2 GUIDING PRINCIPLES

2.1 The following guiding principles apply:

2.1.1 It is the responsibility of Department Managers to ensure that staff are provided with appropriate equipment, access to and training for the computer facilities required to perform their function.

2.1.2 Every individual has a responsibility to exercise good information security practices and common sense in using the Company's computer facilities.

2.1.3 All information contained on the Company's PCs and servers remains the property of the Company and the information will be monitored on a regular basis to ensure the guiding principles are being observed.

3 DEPARTMENTAL MANAGERS

3.1 Responsibility for determining the computer requirements for all staff rests with Department Managers, as follows:

3.1.1 Equipment. The organisation of the provision of appropriate computer equipment and the software required is the responsibility of the Department Manager.

3.1.2 Access Control. Human Resources (HR) will inform ICT services of all new starters and leavers. Under the guidelines contained in the Access Control Procedures, it is the responsibility of Department Managers to advise ICT services of the access required, and of ICT services to ensure that the agreed levels of access for any one individual are not being exceeded. In this eventuality, ICT services is to discuss the issue with the Department Manager and seek a resolution. If this is unsuccessful, ICT services is to raise the matter with Audit, who will then take appropriate action.

3.1.3 Internet Access. Internet access on the employee's PC will be provided where there is a clear business need, as documented by the Department Manager and agreed by the Head of e-Business, who will maintain a central log.

3.1.4 Monitoring. Department Managers are to check that these information security guidelines are followed and to show leadership in respect of observing the guidelines themselves.

Turn over ▶

4 INDIVIDUAL INFORMATION SECURITY

4.1 All types of security rely upon constant vigilance and common sense by the individual and this applies equally to both physical and information security. The following individual guidelines apply:

4.1.1 Be suspicious of unsolicited e-mails. Although virus-protection software is installed and updated regularly, new viruses can bypass the checking procedures. If you receive an unexpected e-mail from an unknown source, NEVER open any attachments.

4.1.2 Use passwords for secure documents. For any document of a secure nature, an example being a memo containing salary details, always protect this with a password - particularly when sending it as an attachment. It is very easy to accidentally send a document to someone with a name similar to that of the intended recipient. Also, passwords for this type of document are a second level of security should you inadvertently leave your PC unattended or have a laptop stolen from your car.

4.1.3 Sensitive information. On many occasions you will be displaying sensitive information on your monitor. Screen displays can be read from about three metres away by someone with normal eyesight. Be prepared to switch to a different window if you feel staff are showing an inappropriate interest in any material visible on your display.

5 PERSONAL USE OF FACILITIES

5.1 Personal use of the Company's computer facilities must only take place on the PCs provided expressly for this purpose. These will be kept in a location convenient for most departments and their use is permitted on the understanding that it occurs with the consent of the Department Manager and in the employee's own time. This is defined as before work commences, lunchtimes, or after work has finished for the day. This time restriction will ensure that the Company's business will be unaffected and that the networks will not be used for personal purposes during the busy peak times. The following guidelines apply:

5.1.1 Offensive material. Staff must not access any material that could cause offence to others if seen on a screen, or accessed as part of the monitoring procedure (see below).

5.1.2 E-mail use. The Company's e-mail systems are not to be used for personal e-mails but staff are welcome to establish Internet accounts and use Hotmail or similar. There are a number of practical reasons for this. Firstly, staff will be able to read personal e-mails from any Internet PC. Secondly, the cost of disk space and housekeeping of e-mails will become the responsibility of the Internet provider, not the Company. Thirdly, any e-mail sent will not be appended with the Company's statement/disclaimer, thereby avoiding possible problems this could cause to either staff or the Company.

6 MONITORING

6.1 To ensure that the Guidelines are adhered to, ICT services may monitor use of the services in the following ways:

6.1.1 Password violations. Invalid password attempts are recorded and examined to see if someone is persistently attempting to access an unauthorised service.

6.1.2 Internet access. Details of all Internet pages accessed by staff are recorded. Unsuitable pages and those accessed for personal purposes during the peak hours will be investigated.

6.1.3 Use of e-mail for personal purposes. All e-mails sent and received can be accessed and the content read.

Globemob
01/08/2001

END OF CANDIDATE BOOKLET

There is no source material printed on this page