MG ALBA - IT Policy

Introduction

MG ALBA hopes that the following IT policy will lead to the most efficient and safe use of the organisation's IT resources.

By adhering to the following guidelines MG ALBA hopes to:

- protect its IT infrastructure from malicious outside elements.
- protect all systems from damage caused by misuse or careless work practices.
- ensure efficient in-house work practices are adhered to.
- ensure that staff are aware of both the legal and moral obligations surrounding the use of the organisations systems.

Department managers are responsible for the enforcement of this policy within their individual departments.

Failure to follow the organisation's IT policy will be dealt with seriously and appropriate disciplinary action will be taken.

Staff should be aware of their responsibilities under the Data Protection Act, Computer Misuse Act[1] and the Copyright Design and Patents Act. The Operations Manager (ICT) will provide guidance where required.

[1] Computer Users shall not, by any wilful or deliberate act, jeopardize the integrity of the computing equipment, its systems programs or any other stored information to which they have access. Under the Terms of the Computer Misuse Act (1990), unauthorized access to a computer (sometimes called "hacking") or other unauthorized modification to the contents of a computer (such as the deliberate introduction of viruses) are criminal offences punishable by unlimited fines and up to 5 years imprisonment

Approved by the Board on 22/2/18

Part 1 - System Management

Office Network

1. Network management, administration and maintenance within MG ALBA are the responsibility of the Operations Manager (ICT) and/or any organisation holding a system maintenance contract. Access to and usage of the Servers is restricted to authorised staff.

Hardware

2. Any requirement for new office equipment will be assessed by the Operations Manager (ICT).
3. The individual hardware needs of staff members should be brought to the attention of the Operations Manager (ICT), after discussion with Line Manager and completion of appropriate Requisition Forms.
4. The head office infrastructure will be replaced after a preordained period. This will be set by the Operations Manager (ICT) and the Director of Finance.
5. The purchase, installation, configuration and maintenance of computer equipment is the responsibility of the Operations Manager (ICT) and/or any organisation holding a system maintenance contract.
6. Computer equipment registers will be maintained by the Operations Manager (ICT) to ensure full tracking of equipment.
7. The Operations Manager (ICT) will liaise with the Director of Finance to ensure adequate insurance cover for computer equipment. The Operations Manager (ICT) will ensure staff are aware of any restrictions and limitations.
8. The deployment of new equipment or re-deployment of existing equipment is undertaken by the Operations Manager (ICT) after consultation with Department Managers.
9. The security and safekeeping of portable and other equipment used out with MG ALBA offices is the responsibility of the member of staff using it. If any damage or loss is deemed to have been caused by negligence the user may be asked to make reimbursement to the company for the repair or replacement of the item.
10. All members of staff are responsible for the proper usage, care and cleanliness of the computer equipment they use. Managers should ensure that staff maintain the cleanliness of their machines.
11. Problems with office hardware should be reported to the Operations Manager (ICT). If it is deemed that damage has been caused by negligence the user may be asked to make reimbursement to the company for the repair or replacement of the item.

Software & Software Applications

12. The purchase, installation, configuration and support of all software and software applications used within MG ALBA are the responsibility of the Operations Manager (ICT).
13. Software, including screensavers, must not be installed by users without prior authorisation from the Operations Manager (ICT).
14. MG ALBA will treat the installation of unlicensed software by users as a serious breach of the IT Policy.
15. Software licence registers will be maintained by the Operations Manager (ICT) to ensure compliance with legislation.
16. Software disks will be kept securely by the Operations Manager (ICT).
17. Requirements for new software/software applications should be discussed in advance with the Operations Manager (ICT) to assess the detailed specification and implications.
18. Problems with software should be reported to the Operations Manager (ICT).
19. Requests for modifications, enhancements and upgrades of existing software applications should be discussed with the Operations Manager (ICT).

Data Management

20. Data Management should be in accordance with the data management policies and procedures of MG ALBA.
21. Department Managers are responsible for maintaining the quality of the computer-held data processed by their staff.
22. The individual user is responsible to their line manager for the quality of the computer data they have personally processed.
23. Department Managers are responsible for ensuring compliance with Data Protection legislation with regards to data processed within their Departments.
24. In conjunction with the nominated Data Protection Officer of the organisation, the Operations Manager (ICT) will keep abreast of data protection legislation, advise accordingly and ensure applications and databases are registered in accordance with the legislation and internal organisational data management policies.
25. All information/data held on the organisation's systems is deemed the property of MG ALBA.
26. As a condition of employment, staff consent to the examination of the use and content of all data/information processed and/or stored by the staff member on the organisation's systems as required.

Back Up

27. The Operations Manager (ICT) is responsible for ensuring the implementation of an effective back-up strategy for server-held software and data.
28. Users of networked desktop PCs should avoid storing data on their local hard drives. Data so stored may be lost if a problem develops with the PC, and the Operations Manager (ICT) may not be able to assist in its recovery. Staff should use the One Drive for Business application for personal data storage.
29. Employees must ensure that all important corporate documents are stored on MG ALBA's hosted cloud platform (Microsoft SharePoint), within the file directory structure used by the organisation and that said documents are accessible to at least one other member of staff and the Chief Executive.
30. Server held data will be backed up daily with one copy being held off site.
31. Remote and laptop PC users must ensure they back up their data regularly. The Operations Manager (ICT) will provide advice and assistance.
32. Confidential data being carried off the premises via a portable storage device (e.g. memory stick) must be encrypted.

Anti-Virus Protection

33. The Operations Manager (ICT) is responsible for the implementation of an effective virus security strategy. All machines, networked and standalone, will have up-to-date anti-virus protection.
34. The installation of anti-virus software on all machines is the responsibility of the Operations Manager (ICT).
35. The Operations Manager (ICT) will ensure the upgrade of the anti-virus software on networked desk-top PCs.
36. Remote users and users of portable machines will assist in the upgrade of anti-virus software in accordance with specified mechanisms agreed with the Operations Manager (ICT), e.g. internet updates
37. Staff should virus-scan all media (including memory sticks, DVDs and CDs) before first use. The Operations Manager (ICT) will provide assistance and training where required.
38. In the event of memory sticks being used off-site e.g. home, hotels, other companies, the memory stick should be scanned for viruses before it is used again in the office. This should be done by the Operations Manager (ICT) on a stand-alone machine.
39. On detection of a virus staff should notify the Operations Manager (ICT) who will provide assistance.
40. Under no circumstances should staff attempt to disable or interfere with the virus scanning software.

Part 2 - Computer Users

Health & Safety

1. Health and safety with regards to computer equipment and computer work stations should be managed within the context of the general and any specific Health & Safety policies and procedures within MG ALBA. The Office Manager will provide advice.
2. Managers are responsible for ensuring health & safety legislation and procedures with regards to computer equipment are implemented within their Departments.
3. Employees who use Display Screen Equipment will be assessed in accordance with the Health & Safety Policy, paragraph 4.10, and appropriate control measures implemented to mitigate all potential health problems related to design of the workplace, the job, training and consultation.
4. The Operations Manager (ICT) will keep abreast of IT-related legislation and advise accordingly.

Training

5. It is the responsibility of Department Managers to ensure appropriate computer training for their staff is identified. The Operations Manager (ICT) can advise on computer-related training issues.

User Accounts

6. Department Managers should notify the Operations Manager (ICT) of new members of staff in advance to allow the creation of network and e-mail accounts and system permissions.
7. Department Managers should notify the Operations Manager (ICT) of the departure of staff to allow the deletion of network and e-mail accounts.

Passwords

8. The Operations Manager (ICT) will ensure password management is part of the security strategy of the MG ALBA IT system. The Operations Manager (ICT) is responsible for formulating and updating the Password Policy and all employees must comply with the provisions of the Password Policy.
9. Users should change their passwords when prompted by the system in the case of networked machines or on a regular basis for standalone machines.
10. Staff are responsible for the security of their password which they should not divulge, even to colleagues. The Operations Manager (ICT) may need to know passwords to carry out essential maintenance.
11. Problems with passwords should be reported to the Operations Manager (ICT).

System Usage

12. Users should ensure their computers are fully shut down and turned off at least once a week.
13. Computers should be locked or shut down when left unattended for any significant period.

Approved by the Board on 22/2/18

Part 3 - E-mail & Internet

E-Mail

1. The MG ALBA e-mail system should not be used for political, business or commercial purposes not related to MG ALBA.
2. The MG ALBA e-mail system must not be used to send illegal or inappropriate material.
3. Limited personal use of email is permitted. Managers should ensure there is no abuse of this privilege.
4. Global distribution lists should be used appropriately. Email to all staff (spamming) should be used only when appropriate.
5. Staff should minimise the number of messages in their email in-box to ensure maximum efficiency of the delivery system. Folders should be set up and messages filed accordingly.
6. Staff should utilise the archiving facility within the Email system in accordance with current guidelines.
7. Confidential material sent by e-mail should be so marked but sent only with caution.
8. MG ALBA retains the right to access and view all Emails sent and received by the Email system. This right is exercised solely through the Operations Manager (ICT) on the instructions of the Chief Executive.
9. Staff should only divulge their email address to trusted parties, failure to do this may lead to a significant increase in spam email.
10. Do not broadcast email addresses to other organisations. If you are forwarding a message to both staff and outside parties, the blind carbon copy (bcc) option should be selected.
11. Do not open any emails that you are not completely sure about. If you have any doubts about the content of an email contact the Operations Manager (ICT).
12. If the supply of an email address is essential in any given transaction, and you are not dealing with a trusted supplier, it would preferable if the user supplied a disposable email address e.g. Hotmail, Yahoo or Google Mail.

Internet

13. Access to the Internet is provided for business purposes. Limited personal use is permitted as long as it does not incur specific expenditure for MG ALBA, impact on job performance, break the law or bring MG ALBA into disrepute.
14. Staff should not make inappropriate use of their access to the Internet. They must not use MG ALBA systems to access pornographic, illegal or other improper material.
15. Staff should not subscribe to chat rooms, dating agencies, messaging services or other on-line subscription Internet sites unless they pertain to work duties.
16. Programs, including screensavers, must not be downloaded from the Internet without authorisation from the Operations Manager (ICT).
17. MG ALBA retains the right to monitor Internet usage by staff. This right is exercised solely through instruction by the Chief Executive and where relating to a specific member of staff. This will be carried out by the Operations Manager (ICT).
18. It is a condition of employment that all staff consent to the examination of the use and content of their Internet activity as required.
19. Abuse of Internet access will be dealt with relative to seriousness. Minor abuse may lead to removal of internet access from an individual's workstation. More serious breaches will be dealt with in accordance with MG ALBA's disciplinary procedures.

I hereby acknowledge receipt of a copy of MG ALBA's IT Policy.

I accept the policy and fully understand that failure to adhere to this policy may lead to disciplinary action being taken.

Signed by…….

Title……..

Date……..

Approved by the Board on 22/2/18