IT Policy

Introduction

1. The purpose of the IT Policy is to ensure the effective protection and proper usage of the computer systems within Deafblind Scotland (DbS). The IT investment within the organisation is considerable, and the dependency on computer technology in the delivery of DbS services is high. The IT Policy will assist in maintaining systems at operational level. Contraventions of the IT Policy could seriously disrupt the operation of DbS and any breaches will be treated seriously.
2. Managers are responsible for ensuring adherence to the IT Policy within their Departments, overseen by the relevant member of the Senior Management Team.

Section One – Computer Systems

Network

1. Network management, administration and maintenance within DbS are the responsibility of the Chief Executive & Head of Finance, with an IT support contract in place. Access to and usage of the Servers is restricted to authorised staff.

Hardware (Servers, PCs, Laptops, Notebooks, Printers, Modems, etc.)

2. The requirement for IT equipment will normally be identified within the context of an organisational strategy for DbS and more specifically within a planned programme of PC replacement.
3. The purchase, installation, configuration and maintenance of computer equipment are the responsibility of the Chief Executive & Head of Finance.
4. Computer equipment registers will be maintained by Head of Finance to ensure full tracking of equipment.
5. The Head of Finance will liaise with the Chief Executive to ensure adequate insurance cover for computer equipment.
6. Requirements for new hardware should be discussed in advance with the Chief Executive & Head of Finance who will with IT support contractor assess the detailed specification.
7. The deployment of new equipment or re-deployment of existing equipment is undertaken by the Head of Finance after consultation with the Chief Executive.
8. The relocation of hardware within or out-with DbS premises should be discussed with the Chief Executive & Head of Finance in advance to ensure good reason for relocation, determine the most appropriate means of relocation and to ensure computer equipment registers and insurance policies are updated.
9. The security and safekeeping of portable and other equipment used outwith DbS offices is the responsibility of the member of staff using it.
10. All members of staff are responsible for the proper usage, care and cleanliness of the computer equipment they use. Managers should ensure that staffs maintain the cleanliness of their machines.

Reviewed Date: July 2024
Next Review: July 2027

11. All members of staff who undertake hybrid working/working from home must ensure that the new VPN function (virtual private network) is used at all times, allowing all members of staff to establish a secure digital connection between their computer/laptop and DbS server.

12. Problems with hardware should be reported to the Head of Finance by email.

Software & Software Applications

12. The requirement for IT equipment will normally be identified within the context of an organisational strategy for DbS and more specifically within a planned software upgrade programme.
13. The purchase, installation, configuration and support of **all** software and software applications used within DbS are the responsibility of the Head of Finance, who will delegate to DbS IT support contractor.
14. Software, including screensavers, must not be installed by users without prior authorisation from the Head of Finance. This includes programs downloaded from the Internet.
15. DbS will treat the installation of unlicensed software by users as a serious breach of the IT Policy.
16. Software licence registers will be maintained by the Head of Finance and IT support contractor to ensure compliance with legislation.
17. Software media will be kept securely by the Head of Finance in conjunction with DbS IT support contractor.
18. Requirements for new software/software applications should be discussed in advance with the Head of Finance to assess the detailed specification and implications.
19. Problems with software should be reported to the Head of Finance.
20. Requests for modifications, enhancements and upgrades of existing software applications should be discussed with the Head of Finance.

Data

21. Data Management should be in accordance with the data management policies and procedures of DbS.
22. The Senior Management Team and Project Leads/managers are responsible for maintaining the quality of the computer-held data processed by their staff.
23. The individual user is responsible to their line manager for the quality of the computer data they have personally processed.
24. The Senior Management Team and Project Leads/managers are responsible for ensuring compliance with Data Protection legislation with regards to data processed within their area.
25. In conjunction with the nominated Data Protection Officer of the organisation (Senior Management Team), who 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.

Back Up

26. The Head of Finance, devolved to DbS IT support contractor is responsible for ensuring the implementation of an effective back-up strategy for server-held software and data.
27. 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 IT support may not be able to assist in its recovery. Data should be stored within the file directory (folder) structure used by the office.
28. Remote and laptop/notebook PC users must ensure they back up their data regularly. The Head of Finance will provide advice and assistance.

Anti-Virus Protection

29. The Head of Finance, devolved to DbS IT support contractor, is responsible for the implementation of an effective virus security strategy. All machines, networked and standalone, will have up-to-date anti-virus protection.
30. The installation of anti-virus software on all machines is the responsibility of the Head of Finance, devolved to DbS IT support contractor.
31. The Head of Finance, devolved to DbS IT support contractor will ensure the upgrade of the anti-virus software on networked desktop PCs.
32. Remote users and users of portable machines will assist in the upgrade of anti-virus software in accordance with specified mechanisms agreed with the Head of Finance, eg. Internet updates
33. Staff should virus-scan all media (including floppy disks, zip disks, CDs, external hard-drives and memory Stick) before first use. All external hard-drives and memory sticks used require to be encrypted. The Head of Finance, devolved to DbS IT support contractor will provide assistance and training where required
34. On detection of a virus staff should notify the Head of Finance, devolved to DbS IT support contractor who will provide assistance.
35. Under no circumstances should staff attempt to disable or interfere with the virus scanning software.

Section Two – 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 DbS.
2. All staff are responsible for ensuring Health & Safety legislation and procedures with regards to computer equipment are implemented within their areas.
3. The Head of Finance, devolved to DbS IT support contractor will keep abreast of IT-related legislation and advise accordingly.

Training

4. It is the responsibility of Line Managers to ensure appropriate computer training for their staff is identified. The Head of Finance can advise on computer-related training issues.

User Accounts

5. Line Managers should notify the Head of Finance of new members of staff in advance to allow the creation of network and e-mail accounts and system permissions.
6. Line Managers should notify the Head of Finance of the departure of staff to allow the deletion of network and e-mail accounts.

Passwords

7. The Head of Finance will ensure pass-wording is part of the security strategy of the DbS IT system.
8. Users should change their passwords when prompted by the system in the case of networked machines or on a regular basis for standalone machines. All changes to passwords should be notified to Head of Finance as soon as implemented.
9. All passwords should be a minimum of 12 characters, including capital letters, number and special characters.
10. Problems with passwords should be reported to the Head of Finance.
11. You must not violate the privacy of other users on the computer systems
12. For your own security you must not leave your workstation unattended whilst is logged in. Where practical action will be taken against people who leave their station logged in and unattended.

System Usage

12. Users should ensure their computers are fully logged out and turned off at end of day.
13. Computers should be locked or shut down when left unattended for any significant period of time.
14. With regards to file management, Line Managers will determine the top level folders/directories and associated permissions for their department and inform the Head of Finance. The Head of Finance will create or modify the folders accordingly. Within their respective top-level folders, staff should create sub-folders in accordance with DbS guidelines but cannot create new top-level folders.
15. Any member of staff requiring access to restricted information held on the Server should make a request by email to Senior Management team thereafter a standard response will be given to the individual.

Section Three - E-mail/Internet

E-Mail

1. DbS e-mail system is a core business application. It should not be used for political, business or commercial purposes not related to DbS.
2. DbS e-mail system must not be used to send illegal or inappropriate material.
3. Limited personal use of email is permitted. Line 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. If you are 'cc'd' into an email this means you are copied in for information only and should not respond.
7. If you are part of the 'to' email, then you should respond.
8. Archiving will be carried out by IT Consultants on emails beyond a 3-year period. Staff requiring to retain any important emails within this time period should utilise the archiving facility within Office 365.
9. Confidential material sent by e-mail should be so marked but sent only with caution.
10. DbS retains the right to access and view all Emails sent and received by the Email system. This right is exercised solely through the Head of Finance on the instructions of the Chief Executive.

Internet

12. Access to the Internet is provided for business purposes. Limited personal use is permitted and is to be restricted to lunch breaks and periods outwith working time.
13. Staff should not make inappropriate use of their access to the Internet. They must not use DbS systems to access pornographic, illegal or other improper material.
14. Staff should not subscribe to chat rooms, dating agencies, messaging services or other on-line subscription Internet sites unless they pertain to work duties.
15. Programs, including screensavers, must not be downloaded from the Internet without authorisation from the Head of Finance.
16. DbS retains the right to monitor Internet usage by staff. This right is exercised solely through the Head of Finance, and, where relating to a specific member of staff, only on instructions from the Chief Executive.
17. Abuse of Internet access will be dealt with severely relative to seriousness. Minor abuse will lead to removal of the privilege of access from an individual's workstation.

For social media refer to Digital Communication policy

<u>Payment Card Industry Data Security Standard</u>

1. When receiving card payments online payments. No personal data/card information is held within Shared Drives, information is uploaded at time of taking payment through Elavon online. Cardholder data is protected by Dbs firewall and configurations on server. Ie (anti-virus software or programes) when accessing internet.

2. Restricted access to cardholder data and use of Elavon Card Machine, Finance Manager or Finance Assistant

3. Elevon Credit Card Machine to be secure at all times within Finance Office.

Section Four - Contravention of the IT Policy

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

2. Contravention of the DbS IT Policy or any act of deliberate sabotage to DbS computer systems may be considered a disciplinary offence.

[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), unauthorised access to a computer (sometimes called "hacking") or other unauthorised 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