



THE BIRMINGHAM & MIDLAND INSTITUTE

9 Margaret Street
Birmingham
B3 3BS

Charity No. 522852

IT USAGE POLICY

1. General

1.1 Where references are made to internet usage, this applies to all equipment with the facility to gain access to the internet (this includes desktop computers, laptops, and handheld devices such as mobile phones, Smart Phones and Tablets and other PDA that are pre-approved).

1.2 Where “Employees” are referred to in this policy, this covers all individuals working at all levels, including senior managers, trustees, employees and volunteers, consultants, contractors, part-time and fixed-term employees and casual and agency staff.

2. Internet use and access

2.1 The Internet is a worldwide network of computers that contains millions of pages of information. Employees are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material.

2.2 In general terms, it is difficult to avoid at least some contact with this material while using the internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the internet may lead to receipt of unsolicited e-mail containing offensive content. Employees accessing the internet do so at their own risk and The Birmingham & Midland Institute is not responsible for material viewed or downloaded by employees from the Internet.

2.3 The computer network is the property of The Birmingham & Midland Institute and may only be used for legitimate business purposes.

2.4 Access to the internet is only provided to assist certain categories of staff in the performance of their jobs (e.g. marketing & communications, personnel, sales & technical).

2.5 All Employees have a responsibility to use the Institute's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet, may result in disciplinary action, in accordance with the Institute's Disciplinary Policy & Procedure and civil and/or criminal liability.

2.6 It is strictly forbidden to use the internet for private or freelance business, gambling, visiting pornographic and equivalent other entertainment sites, or conducting political activities, including postings to discussion groups, chat rooms, or bulletin boards.

2.7 Without prior written permission from the Institute, the Institute's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g. viruses, self-replicating programs, etc.), political material, pornographic text or images, or any other unauthorised materials. Employees may not use the Institute's Internet connection to download games or other entertainment software (including screen savers), or to play games over the Internet.

2.8 The Institute strictly prohibits the use of social networking, streaming media, shopping, and gambling sites during working hours. Furthermore, you should not post any views, positive or negative regarding the Institute, employees, trustees, members, partners, customers, clients etc. or engage in passing any comment representative of the Institute's views.

2.9 Additionally, employees may not use the computer network to display, store or send (by e-mail or any other any other form of electronic communication such as bulletin boards, chat rooms, Usenet groups, etc.) material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful. E-mail messages must never contain any words, phrases or other material which are sexually or racially abusive and/or are discriminatory, in any way whatsoever, or which may have the effect of the recipient feeling or experiencing harassment as a result of receiving the message. Consequently, improper reference should not be made to race, creed, colour, sexual orientation, nationality, ethnic origin, religion, age, gender, marital status, disability or trade union membership. Anyone who is in receipt of such materials should notify the Honorary Secretary immediately.

2.10 We permit the incidental use of the internet and e-mail systems to send personal e-mail and browse the internet (except for social networking sites as outlined above) subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

The following conditions must be met for personal usage to continue:

- Use must be minimal and take place substantially out of normal working hours.
- Personal e-mails should be labelled "personal".
- Use must not interfere with business or office commitments.
- Use must comply with this policy.

3. Removing Restrictions

The Institute may consider removing restrictions based on business needs and subject to the provision of a robust business case. Any such applications to remove restrictions should be made to the Honorary Secretary, in the first instance.

4. Frivolous Use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all employees connected to the network have a responsibility to conserve these resources. As such, employees must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

5. Use of equipment

Any equipment that is provided by the Institute with internet access must be used as it was intended when provided to the employee. Any employees found to be misusing equipment or using it for excessive personal usage will be subject to disciplinary proceedings under the disciplinary policy and procedure. This includes tampering with any equipment that has been

provided to them, or transferring parts from one piece of equipment to another without authorisation. (e.g. mobile phone SIM cards).

6. Security and confidentiality; Passwords / Logging off / Encryption

In order to protect information and files, all employees must password protect their system and change their password as per internal guidelines and system prompts. Employees must not share passwords.

All 'confidential' information should be password protected or encrypted.

To avoid unauthorised use of email and internet connections, employees should log off when leaving computers unattended.

7. USB Access & Mass Storage Devices

USB access and mass storage device usage may be blocked. Employees will still be able to charge mobile phones but access to storage areas will be blocked. This policy also extends to digital media cards (SD, MMC & other forms of flash media).

8. Illegal Copying

Employees should be careful that they do not infringe any copyright in pre-printed or published material that they incorporate in their e-mails for transmission to third parties for general publication. It is expressly forbidden to copy, download or transmit to third parties any material that has been written by other people without their consent.

Employees are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material they wish to download or copy. They may not agree to a licence or download or install software from external sources without authorisation from the Board of Trustees.

Employees who are concerned, or believe, that an e-mail they intend to circulate may contain copyrighted material, should refer the matter to the Honorary Secretary who should evaluate the e-mail content before it is published or circulated.

9. Virus Detection

Files obtained from sources outside the Institute, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the Institute's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Institute sources, without first scanning the material with Institute-approved virus checking software. If you suspect that a virus has been introduced into the Institute's network, notify the Honorary Secretary immediately.

10. Communication of Institute Information

Unless expressly authorised to do so, employees are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, or other confidential information belonging to Institute. Unauthorised dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties.

11. Logging on at remote locations and other offices

Users who log on from computing devices from remote locations are expected to take due care in where they log on from and should be careful about logging on from public Wi-Fi areas such as coffee shops, hotels and conference locations as these types of locations are vulnerable to Information security threats by eavesdropping and snooping methods.

12. Monitoring of Computer and Internet Usage

The Institute has the right to monitor and log any and all aspects of its computer system including, but not limited to, monitoring Internet sites visited by employees, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

13. Blocking sites with inappropriate content

The Institute has the right to utilise software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

14. Privacy

Employees are given computers and Internet access (where applicable) to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, send or receive using the Institute's computer equipment. The computer network is the property of the Institute and may be used only for Institute purposes.

Employees expressly waive any right of privacy in anything they create, store, send or receive using the Institute's computer equipment (or Internet access). The Institute may access and review all materials created, stored, sent or received by employees through any Institute network or Internet.

15. Personal Devices

Only approved personal devices will be allowed to connect to the Institute resources and will not be exempt from monitoring. Such devices will also only be allowed to access systems on a case by case basis and based on the requested use case and governed by the device's security. Further to this not all systems will be accessible via non-Institute issued computing devices.

16. Email use

E-mail is provided primarily for business purposes and therefore employees should discourage the receipt of personal e-mail. It is recognised however, that email in our society provides an important form of communication and therefore the Institute will accept incidental personal usage. Any employees found to be using the email (or internet where applicable) for excessive personal usage will be subject to disciplinary proceedings under the disciplinary policy and procedure. Employees who have to send personal emails are encouraged to use other internal resources where available e.g. computer access provided in refreshment / café areas.

E-mails should at all times be treated as permanent written records which may be read by persons other than the addressee.

Care should be taken that e-mails are only sent to the appropriate recipients to whom the contents are applicable.

Care should be taken in attaching confidential or commercially sensitive files to recipients. All files must be marked appropriately e.g. "Confidential & Circulation Restricted to [named individuals]" and be appropriately password protected or encrypted.

E-mails written from @bmi.org.uk accounts should always contain the standard footer.

All e-mail accounts should be password protected and only known to the person to whom the account has been created.

17. Content of internal and external e-mail messages

Be aware that when you are using the internet outside of work, you are still representing

the Institute, so you must refrain from any activity that could be considered as discrediting or damaging to the Institute. This includes posting derogatory or harmful comments on social networking or “blogging” sites that could potentially be seen as derogatory to any of the Institute, employees or customers.

Care must be taken that the content or subject matter of the e-mail does not cause offence in any way to the recipient, nor that it is defamatory. In particular, care should be taken as to the style of the language used and the effect the message will have on the recipient. Therefore, the distribution of chain letters, inappropriate humour, explicit language or offensive images is not allowed.

E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user’s inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

Material is defamatory if it has the effect of lowering any person or organisation in the estimation of others. The publication of defamatory material, whether internally or externally on e-mail or the internet, will leave the employee and the Institute open to legal proceedings by the person or organisation concerned. Abuse or misuse of the above provision will result in disciplinary action being taken according to the disciplinary policy and procedure and may result in dismissal.

Unsolicited e-mails must not be opened unless the recipient has a reasonably good expectation of what it contains. If an unsolicited email is received they must delete it immediately.

18. Disciplinary procedures

Employees must note that any breach of any of the provisions of this policy may constitute gross misconduct. The disciplinary policy and procedure will be applied in this event and may in certain circumstances, result in dismissal.

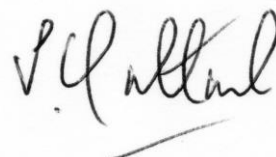
19. Group Responsibilities

All those persons referred to within the scope of this policy are required to adhere to its contents.

The authors have the responsibility for ensuring the maintenance, regular review and updating of this policy. Revisions, amendments or alterations to the policy can only be implemented following the consideration and approval of the Board.



Dr Serena Trowbridge
Vice President



Stephen Hartland
Honorary Secretary

Approved by the Board of Governors: June 2021
Next Review: June 2023