

Introduction:

This document outlines the British Council's policy for the use of its IT equipment, information and systems. The purpose of this policy is to ensure that the British Council's data or reputation is not put at risk through thoughtless or inappropriate use of its information and systems. (Managers are responsible for ensuring all people working for the British Council in any capacity receive a copy of this policy, read and understand it.) Failure to adhere to this policy is a conduct issue and could result in disciplinary action, leading in some cases to dismissal.

1. The British Council filters e-mails for the purpose of detecting spam, viruses and large attachments. It also restricts the use of the internet against inappropriate use, checks software use for licence compliance and telephone logs for inappropriate or excessive use. Any filtering is done by automated tools and is strictly in line with the Information Commissioner's Office guidance: see [The Employment Practices Code: Monitoring at Work](#).

Using business facilities for personal use:

The British Council provides computer equipment for business use; any personal use is strictly limited as follows:

2. Reasonable use of e-mail, the internet or telephones (excluding mobiles) for personal use is acceptable where it does not have a detrimental impact on your work, impact business operations or is used for personal financial gain. For example, using the internet in your normal breaks is acceptable; making personal telephone calls to premium or long distance numbers is not. Reasonable use will be defined by your line manager.
3. Do not use your British Council e-mail address for private business or other commercial interests as the British Council may be seen as entering into the transaction and be legally liable.
4. Do not store personal media files (such as photographs, music, films etc) on British Council equipment including servers. Be aware that the automated software auditing tool gathers details of files stored on portable media devices connected to British Council computers; ensure that no inappropriate material is held on such devices before connecting them.

Working securely:

5. Do not ever attempt to circumvent or defeat security or audit controls unless specifically authorised to do so by the Information Security Team.
6. Do not use words found in dictionaries as passwords as these can be easily cracked. Where possible, use a combination of upper and lower case letters, numbers and punctuation marks to create a pass phrase.
7. Do not write down or give your password to anyone else, including Helpdesk staff or your line manager, as you will be held responsible for any actions taken in your name. If you believe someone else knows your password change it immediately.
8. Do not leave your PC or laptop unattended without locking the screen or logging out. Remember to switch it off at the end of your working day.
9. Inform your line manager if you need any change in access to any British Council IT system. Line managers are responsible for ensuring that their staff have the correct access rights and are removed from IT systems when they leave British Council employment.
10. Inform the Helpdesk or your IT Manager if you suspect someone of trying to access data for which they do not have authorisation.

Appropriate use of software, equipment and information:

11. Do not download or install software from the internet (and that includes Freeware and Shareware). Software must be installed only by authorised staff, and used in accordance with licensing agreements. The use of unlicensed software is illegal and may lead to the British Council suffering serious financial penalties or loss of reputation. Only approved software as listed on the Global Business Services intranet site should be used on British Council systems. If anyone needs specific software because of a disability, please contact Global Business Services to discuss their requirements.
12. Do not copy, download, share or distribute music or video files without the permission of the owner of the intellectual property rights. Business-related media files must not be stored on your personal storage area on the server (usually the H drive).
13. Access to Bit-torrent or other similar peer-2-peer sites using British Council hardware both in and out of the office is strictly prohibited.

14. Do not install, link or attach any equipment to the infrastructure unless this has been specifically approved by Global Business Services.
15. Always scan portable storage media devices (such as USB memory sticks, CDs etc) for viruses or other malicious programs prior to accessing its files. You must always use encrypted portable media devices when taking personal or sensitive data out of the office.
16. Do not make copies of software unless authorised to do so.
17. Do not disclose information belonging to the British Council to any unauthorised third parties; you may only access, copy, amend or delete any information that you are authorised to use.
18. Do be aware that all material (electronic or otherwise) created by or amended by you in the course of your duties while you are working for, or on behalf, of the British Council belongs to the British Council.

Potential loss of data:

19. Do not use local disk drives (e.g. C:\ drive) or portable storage media for keeping sole copies of critical data. The C: drive on your PC is not backed up and may be deleted or overwritten at any time and anyone who logs onto your PC can access data on the C: drive. Keep such data on your server drives.
20. Inform the IT Security Team or your IT Manager of any loss of equipment, personal or confidential information. All personal or confidential information that is taken out of the office in electronic form must be encrypted.

Appropriate use of e-mail:

21. Be aware that the content of e-mails is not private. Any comments you make about an individual in an e-mail or other document may be disclosed to them if they make a request under [Freedom of Information](#) or [Data Protection](#) legislation. In satisfying such requests, the British Council may use back-up tapes to restore e-mails that may have been deleted. The backup tapes for email and data saved to the servers (e.g. G and H drives) are kept for a period of six months.
22. Do not open e-mails or attachments which appear dubious or suspicious. If you are warned of or suspect a computer virus infection, hoax or persistent spam, report it to your IT Manager or email.abuse@britishcouncil.org.
23. Do not reply to unsolicited e-mails (spam) or subscribe to non-business related mailing lists.
24. Do not initiate or forward e-mail chain letters or send out unsolicited joke e-mails; they may offend, be intrusive and be unwanted. Recipients may also perceive them as harassment.
25. Do not send defamatory, abusive or offensive e-mails either internally or externally. Be aware that e-mails are as legally binding as written documents.
26. Do not send emails that imply any religious or political affiliation on the part of the British Council or its members of staff.
27. Do not send attachments larger than 8MB as these can degrade the service for all users of the system. Emails containing attachments larger than 8MB or movie files are blocked at the email gateway.
28. Do not auto-forward your e-mail to external e-mail accounts. You must use an approved remote access system, such as ROAM, or a British Council issued service, like Blackberry, if you need to access your British Council e-mail from outside the office.

Appropriate use of the Internet and Intranet:

29. Do not view or download any pornographic, obscene or offensive material; visit gambling or use auction sites.
30. Do not use audio or video streaming services, play interactive or online games, or visit chat rooms unless these are for approved business purposes.
31. Do not use the British Council logo on personal or non-business related websites as any content, views or opinions expressed may be seen as that of the British Council. Only use the British Council logo if authorised to do so.
32. Whilst using social networking sites, contributing to blogs, wikis etc, please ensure that you:
 - Do not engage in activities which may bring the British Council into disrepute;
 - Do not post unauthorised, private or confidential information;
 - Do not post derogatory, offensive, hateful, inappropriate or obscene material; or attack or abuse colleagues or others;
 - Do not impersonate someone else in order to mislead or confuse.
33. Be aware that internet browsing made via ROAM or a British Council issued Blackberry is monitored as the connection goes via British Council servers.

If you have any questions, queries or comments regarding this policy please contact [Terry Pipe](#) or [Adeoluwa Akomolafe](#)