

Computer Use Code of Ethics

The computing systems at the Bader International Study Centre are intended to support its educational and business purposes and to enhance its educational environment. All Bader International Study Centre computer users should be aware both that they have access to valuable and sensitive resources, and that their computing practices can adversely affect others. This document outlines appropriate and expected computing practices to be followed by all computer users at the Bader International Study Centre.

In the following, "computing facility" includes any personal computer, computing or communications facility owned wholly or partly by the Bader International Study Centre; "account" means any account number, access code, userid, or authorization code for a computer or communications facility, together with its associated passwords and files; "user" means any person using Bader International Study Centre computing facilities; and "system administrator" means a person who has the authority to grant authorization to use computing facilities.

The list below constitutes a Computer User Code of Ethics for the Bader International Study Centre.

1. Users are ultimately responsible for any and all use of their computing accounts. Consequently:
 - a. Users should maintain secure passwords for all accounts assigned to them.
 - b. Users should take precautions against others obtaining unauthorized access to their computing resources (this obligation applies particularly to users who are responsible for confidential information).
 - c. Users should not willingly divulge passwords and other access control information for their personal accounts to any other person.
2. Users must not use or attempt to use computing facilities or accounts to which they have not been granted explicit access by an appropriate system administrator (usually the BISC Computer Support Manager or the BISC Management Team).
3. Users must use computing facilities and services only for the purposes for which they were authorized. Specifically, Bader International Study Centre must not be:
 - a. Used for private consulting or any form of direct personal financial gain (except for appropriate contract and external accounts)
 - b. Sold to any other person;
 - c. Provided as a free resource to other persons for unauthorized purposes.
4. Users must respect all copyrights and licenses associated with Bader International Study Centre computing facilities. Terms and conditions in software licenses can vary considerably. The onus is on users/owners to familiarize themselves with their responsibilities and limitations under each software license agreement. Users must not attempt to:
 - a. Access or use software belonging to or licensed to other users or to the Bader International Study Centre without proper authorization to do so.
 - b. Move or copy programs, sub-routines and any other form of software from one computing system to another without proper authorization. This includes personal computer, microcomputer and personal workstation software.
 - c. Distribute, sell or otherwise make available software when such activity is prohibited by the license agreement for that software
 - d. Access data or information stored on personal or Bader International Study Centre-owned computers without the permission of the owner or custodian of that information.
5. Users must not attempt to interfere with the normal operation of a shared system.

6. Users must not attempt to encroach on others' use of computing facilities or to deprive others of resources.
7. Users must not attempt to subvert the restrictions associated with their computing accounts.
8. Users must not use computing facilities to send obscene, vulgar or harassing messages.
9. Users must not attempt unauthorized access to computing installations outside of the Bader International Study Centre using Bader International Study Centre computers or communications facilities. More generally, users must adhere to all conditions associated with agreements between the Bader International Study Center and external network providers.

Although system administrators may attempt to provide and preserve security of files, account numbers, passwords and programs, it is possible that security can be breached through action or causes beyond reasonable control. Users are therefore urged to safeguard data and to take full advantage of file security mechanisms built into systems (for example by changing passwords as often as necessary). System administrators of shared facilities have a responsibility to inform users of their obligations in the use of these systems.

Alleged violations of the Code shall be dealt with as outlined in the document 'Discipline related to the B.I.S.C. Computer User Code of Ethics'.