



IT Security Issues and Regulations

Policy

The School IT Security Policy applies at all times to:

- Anyone using any IT equipment, including the network or other communication channels on School premises.
- Any member of the School accessing School facilities via network or communications channels from outwith the School.
- You should study these regulations carefully and make sure you fully understand them. If in doubt ask (seepart
- Failures to observe these policies will result in investigation and penalty which may adversely effect your ability to perform your work.

You shall:

- Abide at all times by Scottish, UK, European and international law. This includes all laws pertaining to copyright.
- Abide at all times by the University's Regulations.
- Take note of the specific examples listed in PART I and II below of things that you should **not** attempt to do and are implicitly forbidden within the University regulations.
- Take care at all times to ensure that the integrity of the School is not compromised and to take reasonable measures to ensure that all data including personal identity data is not accidentally or deliberately exposed to anyone.
- If you come across instances where you think security is lax or dubious practices are occurring, please notify the IT team immediately.

PART I Use of any IT equipment within, or access to data and services associated with, the School

This section applies to any use of School facilities or of any personally owned or personally managed computer used within the School premises or any network or communication connections made to the School; ie this section applies to all activities in which the School is in the slightest way associated.

NB: The School network, Edlan and Janet, are NOT to be viewed as a free ISP for personal use. The Janet usage regulations apply [essentially academic use only].

You shall not:

- Connect any device to the network without first following the approval procedures required by the School IT team.
- Provide any networking services for others to use. The machines issued to individual users are configured as client machines to connect to services managed by the School IT team and external providers. You should not attempt to:
 - Operate or run any daemon service without first gaining approval from the School IT Team.
 - Make any channels available whereby data may be accessible to others in a wider remit than the original sources allow.
 - Install or use any "peer to peer" (P2P) file sharing software, eg Gnutella, Kazza, BitTorrent, EDonkey.
- Use the School facilities as a "staging post" between other networks for non academic traffic, eg between a home machine and the Internet.
- Forward chain-letters, pyramid selling or other scam or spam emails.

- It is illegal to download or use any copyright material without prior agreement with the copyright holders, e.g. payment of full license fee in advance.
- It is illegal to distribute software or material in contravention of copyright notices.
- Use the IT facilities (including the network) for any activity other than that concerned with your academic work.

NB: This list is not exhaustive.

Remote and Internal Access

Various Services permit different level of access from different places.

1. Public services, for example the Web servers, are generally available without restriction (although parts of the site are restricted based on either client location or user login).
2. Any system outwith the School, ie in the rest of the University, Resnet and the outside world is considered untrustworthy (no other policy is tenable).
3. There are internal barriers within the School.
4. The inner core is only accessible from certain places by certain users.

The permitted remote access methods require secure user authentication and are by SSL, SSH, SFTP, SCP or VPN only.

PART II: User responsibilities regarding use of PCs provided through the School.

This section applies to any computer system that has been purchased with funds granted to the School irrespective of the original funding source ie systems provided through the School.

- All computer systems supplied through the School are to be under the management of the School IT team unless prior arrangements have been agreed with the School IT Manager.

The list set out below provides examples of activities that users of computers provided through the School, **MUST NOT DO**. To do so will be treated in the same manner as breaching the University's Regulations.

You shall not:

1. Modify firewall rules.
2. Install additional firewalling software (see 14).
3. Install any communications or networking software (see 14).
4. Disable any machine logging (see 13)
5. Modify user account information. This includes:
 - Changing local usernames and passwords
 - Adding additional usernames and passwords
 - Changing user privileges.
6. Attempt to gain "Administrator rights" (MS-Windows) or root privileges (Linux) unless granted by the School IT team(see part
7. Attempt to snoop or determine user passwords.
8. Share your user account information with any other person.
9. Leave a PC on which you are logged in unattended without first logging out or running a password protected screen saver.
10. Open the case to add/remove any new hardware device or modify any existing hardware
11. Modify the BIOS or the BIOS settings, including the BIOS password.

12. (Re-)install the operating system or install additional operating systems.
13. Modify operating system settings or install any software which prevents the system from being managed/monitored by the School IT team.
14. Install or use any software that has not been approved via the Software request and installation service.
15. Store or copy any copyright material without explicit permission from the copyright holder. This includes, but is not limited to, films, music, books, software.

NB: This list is not exhaustive.

PART III Latitude

If any of the items on the above lists specifically hampers your work you need to raise a request through the formal channels provided:

- To use an application, through the application request system.
- Any other matters through SeeSup (the big box at the top of this page!).

NB: Blanket relaxations will **not** be granted, each case has to be made in detail prior to approval being granted. In valid cases, we do expect to grant exceptions but these must be properly requested and assessed in terms of the risk to the School and the data store.

PART IV User Agreement

All users of School facilities are required to agree to these regulations by signing a printed version in duplicate, one copy to be retained by the user, and one by the School.

Any revisions to these regulations will be published on the School's website at <http://www.see.ed.ac.uk/it/security/> and you should familiarise yourself with the amended regulations within 14 days of the publication date. An email notification will be sent to all users during this period.

EASE Username: Name: Sign:. Date:

Reminder from Head of School

"Please may I remind you that the "University Computing Regulations" are designed to help safeguard your reputation and that of the University.

- It is contrary to the "University Computing Regulations" to use the resources of the University, directly or indirectly (e.g. remote access from home), for non-academic or illegal activities.
- It is illegal to download or use any copyright material without prior agreement with the copyright holders, e.g. payment of full license fee in advance.
- It is illegal to distribute software or material in contravention of copyright notices.

I have asked the IT team to attempt to block peer-peer file sharing protocols as little academic justification can be made for using them. The use of peer-peer file sharing protocols either in or via the School is thus forbidden."

27th January 2005