Harlow College IT Network - Acceptable Use Statement.

1. Introduction.

1.1 Anyone using the computer network at Harlow College does so under the conditions imposed by this Acceptable Use Statement. These conditions of use are set for your protection and to ensure the correct operation of the network and the services delivered.

1.2 If you are found to be in breach of these conditions, you will be subject to disciplinary proceedings and your network account will be suspended.

1.3 All network accounts, data storage, computer workstations, Internet and E-mail access will be monitored and regularly scanned for infection by malicious code e.g. viruses, spyware and adware.

2. Acceptable use.

2.1 Any computer related activity by an employee, visitor or contractor, who has been given a network account to use to carry out contractual duties within the boundaries of the Harlow College network and with external organisations accessed via the Internet.

2.2 Any computer related activity by a student, which is limited to those activities required for her/his programme of study and which conforms to current educational best practice.

3. Unacceptable use.

3.1. The deliberate creation, transmission or display, from any source, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

3.2. The deliberate creation, transmission or display of material, from any source, which is designed or likely to cause annoyance, inconvenience or needless anxiety.

3.3 The deliberate creation, transmission, display or other distribution of defamatory material.

3.4 The deliberate creation, transmission or display, from any source, of material such that this infringes the copyright of another individual or company.

3.5 Deliberate activities with any of the following characteristics:
Wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems.
Corrupting or destroying other users' data.
Violating the privacy of other users.
Disrupting the work of other users.
Use of the Internet in any way that denies service to other users (for example, deliberate or reckless overloading of access links or of routing equipment, within and beyond the bounds of the college network).Introduction of "viruses" and any other form of malicious program or code.
Unauthorised installation and/or use of non-college software and hardware.
Unauthorised use of the system facilities to permit one user to masquerade as another user or as a system administrator.
Physical damage or removal of computer resources, hardware, software or datasets.

3.6 To consent to another person using your network identity other than authorised technical support staff, or by allowing unauthorised use by negligence.

3.7 Where the college network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the college network also.

3.8 Use of college computer resources (including consumables such as toner and paper) in pursuit of private business gain.

September 2004, Revised September 2008, January 2009