Regulations for the Use of IT facilities

From all PC workstations in Abingdon & Witney College, it will be possible to access the applications which you need to carry out your work, to store personal files in your own user area and work related files in the shared areas in Office 365 which you can access from any workstation on any site, to send and receive e-mails and to access the Internet.

1. Scope

The following regulations apply to users of all IT facilities owned or leased by Abingdon and Witney College (AWC), all users of such facilities on AWC's premises and all users of such facilities and resources connected to the AWC's networks.

Staff and students should note the consequences of failing to comply with these regulations as set out in the AWC's Handbook and particularly that disciplinary action may be taken by AWC for failure by a user to comply with them and that they may be charged for AWC's costs arising out of such failure

2. Definitions

Users - All staff and students of AWC and others outside the Institution who have been given permission to use the AWC's IT facilities.

Facilities - IT facilities located in AWC's, including networks, servers and personal computers, together with the software and data stored on them. Any IT use carried out on equipment connected to the college network, whether or not this involves the use of a college-based or college-owned computer/laptops.

3. Relevant Legislation

Users must comply with all UK legislation relating to the use of information, computers and networks. Applicable laws include:

a. PREVENT Strategy. Government's counter terrorist strategy

b. Data Protection Act 1998. This act makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. For more information please contact the Head of MIS.

c. Computer Misuse Act 1990. The act provides safeguards for computer material against unauthorised access or modification.

d. Fraud Act 2006. The Act prohibits 'phishing' whereby official-looking emails guide unsuspecting users to fake websites (e.g. fake bank websites) in order to steal their

login details. Creating or possessing software to enable this activity is also an offence.

4. Registration

Authorisation - Use of IT facilities requires prior registration and the granting of a user logon and a individual password. Registration to use IT facilities constitutes acceptance of these regulations. The allocation of a logon and password will constitute authorisation for use of relevant facilities.

Identification - Users must not use another user's code, nor permit any password issued to them to become known to any other person nor, having logged in, leave IT facilities unattended and potentially usable by some other person. Users may not pass themselves off as another person when sending electronic mail or making information available on-line in any other way.

External Users - Use of IT facilities by persons other than staff or students must have the explicit prior permission from IT Services.

5. Use of Facilities and Learning Resources

Personal Use

AWC's IT facilities are provided for educational, administrative, research and personal development use by staff in the course of their employment and by students in the course of their education. Any other use of the college's resources puts an additional demand on those resources, which affects their performance.

Limited personal use of certain facilities is permitted, during personal time. Any such use must neither interfere with the employee's own work or the student's study, nor prevent others from pursuing their legitimate work and use of the college's IT facilities. AWC reserves the right to withdraw this benefit either individually or collectively at any time. In such circumstance AWC will endeavour to give reasonable notice of its intention to withdraw such benefit.

Where AWC becomes aware of a specific type of personal use which affects the efficient operation of its IT facilities, AWC will take appropriate steps to withdraw, without notice, access to the relevant facility.Non-exhaustive examples of this include barring access to certain technology or Internet resources such as web sites, news groups or other Internet resources. Users who have a legitimate requirement to access such withdrawn resources should discuss the matter with IT Services. The fact that a user is able to access a particular technology or resource does not necessarily imply that the technology or resource may be accessed in accordance with these Regulations.

Commercial Use

Use of any of AWC's IT facilities for commercial gain (including advertising) or for work on behalf of others (unconnected with a student's course of study at the College or a member of staff's legitimate activities) is prohibited, unless the User has explicit prior written permission from IT Services.

Movement
AWC IT facilities should not be moved or disconnected without the prior agreement from IT Services.

Connection - Network Access
Users must not connect any device into the AWC's network or other IT facility without prior agreement from IT Services.

Damage
Users must not cause any form of damage to AWC's IT facilities, software, or to any of the rooms and their facilities and services which contain that equipment or software. The term 'damage' includes any unauthorised installation of hardware or software, which incurs time and/or cost in restoring the facilities to their original state.

IT Security
Users must not deliberately introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into any IT facility, nor take deliberate action to circumvent any precautions taken or prescribed by the College to prevent this. Users must not attempt to penetrate the security and/or privacy of other users' files.

Spam and Mass-circulation
Spam is usually defined as unsolicited electronic messages (using email, SMS, Instant Messaging or other means) sent in bulk. Users may not use AWC's IT facilities to send Spam.

Illegal and/or Offensive Material
Users must not use AWC's IT facilities to access, produce, obtain, download, store, view, share, or distribute material (including images, video, text or sound files) which is either illegal under UK law (e.g. in breach of copyright law) and/ or can reasonably be judged to be offensive, likely to incite racial hatred, obscene, indecent, or abusive. The only exceptions would be where such material, which may be judged offensive, is essential for research or teaching, is permitted by law, and prior written permission has been granted by IT Services.

Discrimination
Users must not use AWC's IT facilities to place, disseminate or receive materials which discriminate or encourage discrimination on, for example, the grounds of gender, sexual orientation, disability, age, religious belief, race or ethnic origin.

Defamation Users must not use AWC's IT facilities to publish any information which they know or believe to be untrue

Is defamatory and could not be defended on the grounds that it is true/factual or that it is fair comment on a matter of public interest (e.g. works of literature, art, music, television and radio or the activities of public figures)

Internet Safety
Users to be aware AWC promote Internet Safety. Links to government run websites are available on the AWC Office 365 site.

6. Behaviour

Users must not interfere with or disrupt the availability and use of the IT facilities by others. Users must take every precaution to avoid damage to equipment caused by the presence of food and drink in its vicinity.

Users must also comply with any further specific instructions or regulations displayed alongside IT facilities or on computer screens.

7. Infringement

Withdrawal of facilities - If a User is in breach of any of these regulations, the IT Services may withdraw or restrict the User's use of IT facilities, following consultation with the User's Head of Department or Head of Faculty.

Removal of Material - AWC reserves the right to remove material from its IT facilities without notice where such material is in breach of these regulations.

Disciplinary action - Any breach of the regulations may be dealt with under AWC's formal disciplinary procedure for students and staff and in some cases may result in expulsion or dismissal. The User may be charged for any costs that have arisen as the result of misuse or abuse of facilities.

Breaches of the law - Where appropriate, suspected breaches of the law may be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction

8. Monitoring of IT Facilities

In order to protect the security and working of AWC's IT facilities, it may be necessary to monitor collective or individual usage of its IT facilities. This is particularly likely where there are indications of abuse of systems, or that individuals may be using systems in excess of their authority. Files, messages and user account information may be intercepted, monitored, recorded, copied, audited, and inspected. This information may also be disclosed to authorised AWC's staff and to the police.

Such investigations will only be carried out with the agreement of the Deputy Principal, Vice Principal , Head of Department and Head of Faculty.

Related College Policies

IT user regulations Data Protection

Procedure History

Policy/Procedure Title	IT Use of Systems Regulations
Issue Date	September 2019
Author (Name/Department)	Lee Reszeter, Head of IT Services
Review Date	September 2022
Issue Number	4
Impact Assessed	Yes - September 2019