

WINCHESTER COLLEGE

ACCEPTABLE USE POLICY (AUP)

Introduction

We assume that parents will ensure that their sons read this Policy before coming to school in September. There is a copy for them in a separate envelope contained in this package.

Please see the paragraph on **Personal Computers and JP** on page 8 of this booklet.

The use of Winchester College ICT resources and services is a facility granted, at the School's discretion, to pupils. This Acceptable Use Policy is essential for managing and sustaining the integrity of the Winchester College network and all computing resources that Winchester College makes available.

The purpose of this policy is to define responsible use of Winchester College ICT resources and services, and to minimize legal risks to Winchester College through the use of those resources and services, not to enumerate exhaustively all possible requirements and obligations.

For the purpose of this document, the term "resources" is employed for all hardware, software and media provided by Winchester College, and the term "services" is employed for the use of the Intranet, Internet, file services, data and email.

- Use of Winchester College ICT resources and services constitutes agreement to comply with this policy. The consequences of breaching the AUP may include dismissal.
- These rules apply to the use of any of the school computers, wherever they may be. They also apply whenever a user is logged on to the Winchester College Intranet or network or otherwise using a computer on the school campus.
- The AUP is an extension of the School Rules and the Winchester Code. The rules regarding courtesy and good behaviour; and the terms of the Anti-Bullying Policy and those of the Protocol for the use of mobile telephones at Winchester are also relevant in this connection.

Wincoll local Pupil User Accounts

Winchester College maintains a Microsoft Windows Server 2003/XP (now migrating to Server 2008/Vista) network for administrative and curricular requirements. Students are given a user account to enable them to use the facilities on the Wincoll.local domain, including a 'My Documents' folder on a file server. Use of this account is monitored – it is neither private nor privileged. Files stored by a user may be accessed by teaching staff and ICT Services. The School cannot accept responsibility for a pupil's loss of data whatever the cause. It is the pupil's responsibility to ensure that adequate backups are made.

Wincoll.ac.uk email Services

Winchester College maintains email services for teaching and other staff. Pupils are given an e-mail account to use in the form of their *logonname@wincoll.ac.uk*. This email is monitored and filtered – it is neither private nor privileged.

The user is responsible for the content and maintenance of his or her electronic mailbox.

Remember:

- Check email daily and remain within your disk quota.
- Keep messages stored in your mailbox to a minimum.
- Do not distribute an image of any person via the network.
- Follow the generally accepted rules of network etiquette. These include, but are not limited to, the following:
 - Be polite and use appropriate language. Do not swear or use vulgarities. Do not bully.
 - Do not reveal your personal address or telephone number, nor the personal addresses or telephone numbers of others.

Personal Computers

A JP pupil with properly documented educational needs, a VIBk entrant and any other boy from the beginning of the Common Time of his MP year may be allowed to bring a laptop into his House at the discretion of his Housemaster. Only with the express written permission of both the Housemaster and the Head of ICT Services may a computer other than a laptop be brought into the School. Subject to his strict adherence to the AUP, a pupil may enjoy the use of the Internet connection available through the campus area network. This privilege may be withdrawn without notice at any time.

Inspection of Personal Computers

Personal computers and any storage-media that are under the control or in the possession of Winchester College pupils may be examined by ICT Services staff at any time. Such machines may be removed for the purposes of such an examination. Examination may include inspection, backing up, imaging or copying all or part of the hard drive(s) of such machines, as well as obtaining print-outs of files, logs, caches and data on the machine.

Removal and examination are carried out with the Headmaster's authority. The pupil is expected to co-operate in this matter, but the School does not need his permission to take such action. At least two members of staff will be present throughout the examination. Where possible the pupil will be invited to be present except where this may frustrate the purpose of the examination. The pupil must give account logon names and passwords when these are requested.

Winchester College Network Security

1. You must not use someone else's username to gain access to the School network.
2. You must not write down or otherwise record your password, nor share your password with another.
3. You may not attempt to circumvent user authentication or security of any host, network or account, or penetrate security measures ("hacking") on, related to, or

accessed through the Winchester College network. This includes, but is not limited to:

- a) accessing data not intended for you;
 - b) logging into a server or account which you are not expressly authorized to access;
 - c) falsifying a username or password, key-logging, unauthorized use, or forging, of mail header information (“spoofing”);
 - d) probing, scanning or testing the vulnerability of the network or other networks, and executing any form of network monitoring which will intercept data not intended for the user;
 - e) malicious email, including, but not limited to, mail-bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
 - f) port scanning, ping flood attacks, packet spoofing, forged routing information, deliberately attempting to overload a service and otherwise attempting to “crash” a host.
4. You must not use the network to access or process pornographic material, inappropriate text files, or files dangerous to the integrity of the network.
 5. Hate mail, harassment, discriminatory remarks, and other antisocial behaviours are prohibited. You must not transmit, re-transmit, distribute, publish, promote, market, or store material on or through the Winchester College network which:
 - a) is bullying, threatening, abusive, hateful, obscene, indecent, or defamatory;
 - b) involves or encourages conduct that may constitute a criminal offence;
 - c) constitutes a copyright infringement; or
 - d) involves the transmission, distribution, or storage of information or data which breaks any law or which contains a virus.
 6. You may not connect a Wireless access point to the network.
 7. You must ensure that an anti-virus program is installed and running on your personal computer before it is connected to the network.
 8. The Winchester College Data Protection policy must be observed at all times.
 9. Winchester College will investigate incidents involving breaches of the AUP and may involve and will co-operate with the Police if a criminal act is suspected. Winchester College maintains the right to determine whether specific uses of the network are consistent with acceptable practices.

Revised May 2010