



Handsworth Wood Girls' School

ICT Acceptable Use Policy

October 2010

Staff Acceptable Use Policy

This policy covers the use of all school computer equipment, hardware and software, the School Network.

Section A - Computer Facilities

1. Overview

At Handsworth Wood Girls' Visual and Performing Arts Specialist College and Sixth Form Centre, we allow all staff and students access to our computer network, enabling them to use standard applications (word processing, spreadsheet, database etc.) as well as online facilities such as the Internet, intranet and electronic mail. Every member of staff and student is issued with a username, password for the school network and a username, password and an e-mail address. Students are encouraged to make use of ICT facilities in support of their studies in all subjects, including the writing up of coursework assignments and other projects. Teaching staff are encouraged to make use of ICT to support teaching and learning, thus providing a variety of opportunities in the classroom to engage all students.

All users of the school network and ICT network must ensure that their usage of ICT is both ethical and appropriate. Failure to comply with the rules, which govern the use of the network and ICT equipment, is classed as a serious offence and action will be taken against the individual and this may result in access to computer equipment being withdrawn for a specified period of time and for students even an exclusion.

The school provides a network environment in which users can assume that their legitimate use of computers and the data that they store are secure against interference by other users.

Users should not, however, assume that their activities are completely private. All network, Internet and usage on all of the schools ICT equipment is monitored both in school and out of school. The school monitors user accounts, fileserver space and ICT activity as judged necessary. Hence, records of computer activity, files that have been stored, and e-mail messages that have been sent or received may be scrutinised by the members of staff responsible for management of the network either:

- (a) During routine system maintenance, or
- (b) If there is reason to suspect misuse of the network.

In addition to this the school has software that records misuse of the ICT equipment and network and records date and time stamped screenshots of these violations.

2. Rules

The following rules apply in all the areas of the school where computers are provided for usage, to all of the school's ICT equipment and to all users.

a. General Conduct and Use

- i. No food or drink may be consumed in an ICT facility.
- ii. Any damage to computers, furniture or fittings should be reported to a member of the ICT support staff without delay. The same applies to any apparent malfunction of equipment.

b. Use of the Network

- i. When logging on to the network, a user must always use their own user identification and password. Any attempt to impersonate another user will be treated as a serious offence, as will any attempt to interfere with data stored on the network by another user. **These activities are in fact illegal under UK law.**
- ii. Never, under any circumstances, use another person's account or attempt to log on as a system administrator.
- iii. Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user. The school network or other networks connected to the Internet must not be vandalised. This includes the uploading or creating of computer viruses.
- iv. Harassment is defined as the persistent annoyance of another user, or interference with another user's work. Harassment must never occur; this includes, but is not limited to, the sending of unwanted email.
- v. If you feel you can identify a security problem on the school system you must notify one of the ICT support staff immediately. You must not demonstrate the problem to other users.
- vi. Users must never divulge their passwords to anyone else. Any user who suspects that this has happened accidentally should request from the ICT support staff that their password be changed without delay. All staff users will be required to change their password every 30 days.
- vii. Before leaving a computer, users must always log off the network and check that the logging out procedure is complete.
- viii. Users must not attempt to gain access to the local drive of any machine other than when the user is a member of staff and the machine they are using is their school laptop or to create local accounts (administrative or otherwise).
- ix. Only software that has been provided on the network may be run on the computers. Users are not permitted to import or download applications, music or games. In many cases it is illegal to do so.
- x. You are reminded that it is a breach of School Policy (and of the rules of examination boards) to pass off another's work as your own. This also applies to information accessed electronically as it does to that gained in other ways. If work is copied you will be at risk of having ALL of your coursework and examinations nullified.

c. Use of Staff Laptops

- i. Each member of the teaching staff will be supplied with a laptop. **This remains the property of the school and must be returned to the school if a member of staff leaves.**
- ii. All staff supplied with a school laptop must ensure that it is brought into school every working day. It is the member of staff's responsibility to ensure that their home insurance covers the laptop from theft or accidental damage whilst it is at home.
- iii. If the laptop is stolen within school, then it must be reported immediately to the Dr Hylands. If it is stolen outside of school, the member of staff concerned must report it to the police in order to obtain a crime reference number.

- iv. If the laptop is accidentally damaged, then the member of staff concerned must report it to the ICT technical staff immediately who will try to carry out the necessary repairs. If this is not possible, then a replacement will be considered and may involve a delay.
- v. **Storing and viewing or accessing websites that contain inappropriate material or participating in illegal activity such as downloading copyright music and films may constitute Gross Misconduct, even if this is done out of school on school equipment.**
- vi. Staff must not allow other people to use their School laptop and do so at their own risk.
- vii. The use of peer to peer file sharing software such as Limewire is not allowed.
- viii. Staff should check their school email accounts at least twice daily, a.m. and p.m.
- ix. Staff have a responsibility to take reasonable care to ensure the security of the laptop at all times, for example locking their classroom when they are not present.
- x. Staff agree to follow all guidelines set in the Laptop Agreement when the laptop is issued.

Section B - Internet and E-mail

1. Overview

The School's Internet access is provided by BCC Broadband which deny access to web sites known to contain offensive or inappropriate material. The filter is continually updated, though there can be no absolute guarantee that unsuitable material is never available to users.

Students are given training in effective use of the Internet as a research tool at various stages throughout their School career.

Please refer to the School's Internet Usage Policy for further detail.

Responsible Internet Use

a. Rules for Staff and Students

- i. The school computer system provides Internet access to students and staff. This Responsible Internet Use statement will help protect students, staff and the school by clearly stating what is acceptable and what is not.
- ii. Access must only be made via the user's authorised account and password, which must not be given to any other person.
- iii. School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- iv. Staff or students should not try to bypass the school or local authority's security settings to gain access to material that has not been allowed.
- v. Copyright and intellectual property rights must be respected.
- vi. Users are responsible for e-mail they send and for contacts made.
- vii. Staff must use their school email address for all email correspondence related to their job. Personal e-mail accounts must not be used.
- viii. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. The use of all upper-case text in either the subject or the body of an e-mail should also be avoided as this is deemed to be the e-mail equivalent of shouting;

- ix. Messages should be clearly addressed to those from whom an action or response is expected, "cc" or "bcc" should be used for other recipients of the message;
- x. Use 'reply all', 'ALL STAFF' and distribution lists with caution in order to keep the number of your messages to a minimum and reduce the risk of sending messages to the wrong people;
- xi. Anonymous messages and chain letters must not be sent.
- xii. The use of public chat rooms is not allowed.
- xiii. The school ICT systems may not be used for private purposes, unless the Headteacher has given permission for that use.
- xiv. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- xv. The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- xvi. Irresponsible use may result in the loss of Internet access or more serious sanctions may be taken dependant upon the seriousness of the violation.

b. Personal Safety

In addition, users need to be aware that thoughtless use of e-mail and the Internet may jeopardise their personal safety either at school or outside school. Pupils should therefore:

- i. Never arrange a meeting in person with anyone they have "met" or only communicated with by computer, without prior parental approval.
- ii. Not respond to messages or bulletin board items that are indecent, suggestive, belligerent, discriminatory, threatening, or which make the student feel uncomfortable or unsafe in any way. If such a message is encountered the student should report it to their form tutor and parents.
- iii. Be aware that any person they "meet" or communicate with online may pretend to be someone else.
- iv. Remember that anything they read online may not be accurate.
- v. Ignore offers that involve either financial transactions or personal meetings.
- vi. Not disclose any personal details, such as their home address or telephone number, across the Internet.

I agree to abide by the above

Name:

Signature:

Date:

Department:

This policy has been prepared with reference to the SCC Dyslexia Friendly guidelines and will be reviewed annually.

Acknowledgements

We would like to thank the members of the ICT Strategy Group who have provided huge assistance in the development of this whole school guide.

Signed:

Date:

Dr. Kevin Hylands
Deputy Headteacher (Director of Curriculum and Assessment)

Adopted and Agreed at the Governors Curriculum and Policies Meeting

Signed:

Date: 16th May 2011

Mrs. Brenda Addison
Chairman Curriculum and Policies Committee