Handsworth Wood Girls' School

Laptop Policy

November 2011

Handsworth Wood Girls' School

Portable Computer Issue Agreement And Acceptable Usage Policy

Name of Person Issued To:

Date Issued:

1. Introduction

This document comprises the IT Security policy, acceptable usage policy and equipment issue agreement for portable or mobile computer systems as described below and supplied by the Handsworth Wood Girls' School (HWGS) IT Support department. Non-HWGS purchased Portable Computers must not be connected to the HWGS network unless authorised by IT.

For the sake of this document Portable Computers are defined as Laptop, Notebook and Netbook computers and electronic notepads. The security of other digital devices such as PDAs, Palmtops, and Advanced Mobile Phones etc. is NOT covered by this document.
This document works in conjunction with the main HWGS computer usage access policy. This document is subject to review.
Only authorised persons are allowed access to and use of the Portable Computer Systems. Persons accessing data and using it for educational purposes should afford all material stored and processed on these systems adequate protection. Please consult IT Support for advice.
Portable computers are for conducting school work and while it is acceptable to take them home **they must always be available for use during the school day**. Staff who are unable to transport portable computers between work and home must leave them in a secure place on the school premises overnight such as a locked cupboard or storeroom.

2. Ownership of Equipment

Any Portable Computer issued to you under this policy remains the property of Handsworth Wood Girls' School. On termination of employment or for extended absences such as maternity leave, Handsworth Wood Girls' School will require the Portable Computer and any accessories to be returned. Handsworth Wood Girls' School reserves the right to demand the Portable Computer be returned at any time. A maximum of 7 calendar days is acceptable between the request to return the Portable Computer and it being returned.

3. Physical /Hardware Security

The user of the Portable Computer should always adhere to the following guidelines:

- The Portable Computer must be securely locked away when not in use.
- Portable Computer security is your responsibility at all times.
- If you have and use a Portable Computer security cable, keep one key with you and the other in a secure separate location. A security cable can be requested from IT Support.

- Do not leave the Portable Computer unsecured and unattended in a public place; this includes areas such as the staff room and assembly halls.
- Do not leave the Portable Computer in view inside of your car. Please lock it away in your car's boot.
- Avoid leaving the Portable Computer within sight of ground floor windows or within easy access of external doors, unless secured.

4. Virus and Spyware Control

The Portable Computer System will have an Anti-Virus software package installed by IT Support. Users are not to alter the configuration of this package unless express permission has been obtained from IT Support. The anti-virus system's database of virus definitions must be updated on a regular basis, each day if possible, but at least once a week. To update your virus definitions then it is necessary to connect to the network, either wired or over a wireless connection. This package has been installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.
If a virus is discovered the following actions must be carried out:

- Turn the Computer off
- Isolate any Floppy disks or USB memory sticks that have been used on that machine
- Inform IT Support as soon as possible

IT Support will have the software and technology available to eradicate any infections and recover infected files if possible.

5. Password Security

Password Security is the responsibility of the individual. Passwords should be formulated in such a way that they are easily remembered but difficult to guess and should be formulated using letters (upper and lower case), figures and other characters.

- When allocated a new/temporary password for start-up use by IT Support the user must immediately change it.
- Passwords must consist of a minimum of 6 characters and for strong passwords should also include 2 numerics as part of the 6 characters.
- Passwords must not be shared amongst users. Any malicious or questionable activity detected under a user account will be attributed to the account owner.
- Passwords must not be written down.
- Passwords should not relate to the system or the user, although passwords must be easy to remember.
- Passwords should be changed regularly, at intervals not exceeding 90 days.
- Sensitive student data should not be kept on unencrypted hard disks or USB drives to prevent others accessing this data should the Portable Computer be lost or stolen.

6. Internet/e-mail

The Personal Computer has been provided by the organisation for use on and off site. It should be noted that the Internet is an uncontrolled, unmanaged and largely unsupported global network. It is a source of much valuable information; however it is also an unrestricted source of much illegal and illicit material.

Additionally it has a large recreational attraction. Please see Handsworth Wood Girls' School policies covering Internet and Email usage.

7. Maintenance

- Please do not drop or bump your Portable Computer
- Please do not place heavy objects on the case
- Please do not touch the screen
- Do not use any other power pack than you were assigned
- Do not disassemble your Portable Computer
- Do not clean the screen with anything other than a damp cloth. Please see IT Support for advice on this.
- Take care of network cables as the connectors can be easily broken
- Always turn off your Portable Computer before storing it in its travelling bag for extended periods
- Avoid subjecting the Portable Computer to extremes of temperature, for example leaving it in your car during hot days or cold nights
- Please keep all liquids away from your Portable Computer.

Maintenance is to be controlled by IT Support in conjunction with external suppliers. From time to time your laptop will be recalled by IT Support for maintenance purposes. It will not be possible to properly support the laptop until it has been returned for maintenance.   If the Portable Computer requires external repair, all data will be removed from the laptop ahead of repair.

8. Backup

Work should be backed up regularly to the school network. This can be done by connecting to the school network before logging in, then copying work to your home directory located within "My Computer". Work should not be stored on USB drives. These are purely a method to transfer work between machines. If work is lost due to a damaged or faulty USB drive it is unlikely that IT Support will be able to recover work from it without significant cost, which will be charged back to the department in question.

9. Accounting and Audit

The software and information held on Portable Computer Systems is subject to the same audit procedures as the desktop/tower Computer Systems. This also covers information and data stored on removable media e.g. floppy disks and USB pen or sticks. All software on school computers must be correctly licensed, otherwise it will be removed to comply with the law.

10. Losses and Confidentiality/Security Breaches

All incidents that constitute a Loss of Hardware or Data, which could potentially lead to a breach of Student or Staff confidentiality, are to be reported to the Network Manager and the Deputy Headteacher, as soon as possible after the incident occurs. The Network Manager will instigate investigation procedures to try and establish the nature and potential threat of the incident.
Incidents could involve:

• Loss of Hardware. • Loss of Software/Data. • Virus attack	• Unauthorised access. • Misuse of System/Privileges. • Illegal software download

11. Legislation

Users of portable systems must comply with current legislation regarding the use and retention of Student information and use of computer systems.
These include, but are not limited to:

- The Data Protection Act, 1998.
- The Copyright, Designs and Patents Act, 1988.
- The Computer Misuse Act, 1990.

12. Software Security

Users of Portable Systems are allowed to request administrator rights for the Portable Computer issued to them. However, it is recommended that staff do not have administrator roles as it makes the Portable Computer more susceptible to infection from Viruses, Trojans, Spyware and Scareware.
Users without administrative rights who require additional licensed software to be loaded should contact IT Support or log a request through the help desk.
Users who request and are given administrative rights should adhere to the following rules.

- Only install freeware or shareware software that is relevant to teaching.
- All software that requires a license must be purchased and installed through the ICT Technical Department.
- Non-HWGS purchased software must not be installed on the Portable Computer.
- Ensure that the Portable Computer is connected to the school network at least once a week to update the anti-virus software.

Software obtained illegally should not be loaded onto Portable Computer Systems.
Staff found to be in breach of the above rules will receive a warning on the first occasion and will have all administrative rights removed upon a second breach. Any breach considered to be inappropriate may result in the member of staff facing a formal disciplinary.

I agree to abide by the above

Name:

Signature:

Date:

Department:

13. Administrative Rights

I have read and understood section Software Security Policy detailed in Section 12 of the Handsworth Wood Girls' School Portable Computer Issue Agreement and Acceptable Usage Policy and would like to request Administrative Rights for Portable Computer being issued.

Name:

Signature:

14. Portable Computer Information **Make:**

Model:

HWGS Asset Number:

Serial Number or service tag:

Additional Hardware Issued:

Additional Serial numbers:

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