



# ***Computer Resources Policy for Students and Staff***

**Recommended by:**

**Resources & People Committee**

**Date: 15 October 2015**

**Adopted at Full Governing Body Meeting**

**Date: 24 November 2015**

**Signed by R J Collis DL, Chair of Governors:**

**Review date: Autumn Term 2019 (earlier if any legislative change)**





# The Cottesloe School

30 November 2015

*Please sign and return this form as soon as possible, and keep the attached document for future reference*

**To: Mr A McBurnie, Headteacher**

I confirm that I have received a copy of The Cottesloe School's E-Safety Policy, which was agreed by the Teaching, Learning and Achievement Committee on 7 October 2015 and adopted by the Full Governing Body on 24 November 2015.

## STAFF INFORMATION SYSTEMS CODE OF CONDUCT

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to read and sign this code of conduct. Staff should consult the attached E-Safety Policy for further information and clarification.

- The information systems are School property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that School information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the School may monitor my information systems and Internet use to ensure Policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in School, taken off the School premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to a member of the School's Safeguarding Team via the confidential CP database.
- I will ensure that any electronic communications with students are compatible with my professional role.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The School may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the School's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed .....

Name .....  
(Block Capitals)

Date .....



# COMPUTER RESOURCES POLICY FOR STUDENTS AND STAFF – SEPTEMBER 2015

## Student Guidelines

The school has provided computers for use by students. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Students are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

### **Equipment**

- **Do not** install, attempt to install or store programs of any type on the computers without permission.
- **Do not** damage, disable, or otherwise harm the operation of computers, or intentionally waste resources. Where hardware is found to have been willfully damaged, the school will seek to recover the cost of a replacement or repair from the student.
- **Do not** use the computers for commercial purposes, e.g. buying or selling goods.
- **Do not** connect any non-school mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) without the prior permission of the Business Manager.
- **Do not** eat or drink near computer equipment.

### **Security and Privacy**

- **Do not** disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number, your school's name, or send them your picture, unless you are given permission to do so.
- **Do not** use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and memory sticks/devices will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly.

### **Internet**

- **Do not** access the Internet unless for study or for school authorized/supervised activities.
- **Do not** use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- **Do not** engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone unless your parent/guardian or teacher goes with you. People you contact online are not always who they seem.

### **Email**

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,

- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff.

### **Access to computer resources**

Although the Library incorporates a Sixth Form study area, it is also available to all students at break and lunchtimes for quiet reading and use of laptops for homework and research.

### **VLE - Terms of Use**

When using the VLE and connecting services users must

- Respect the rights of others.
- Remember to logout at the end of each session.
- Comply with current and future legislation including:
  - The Data Protection Act 1998
  - Copyright, Designs and Patents Act 1988
  - Telecommunications Act 1984
  - Protection from Harassment Act 1997

The following are not permitted at any time

- The creation, display, production, storage, circulation or transmission of pornographic or other offensive material in any form or medium (including sending, posting or displaying offensive images, language or any other type of offensive content including the bullying, harassment and intimidation of others.
- Users must not create, store or transmit:
  - Defamatory or libelous material
  - Material that infringes copyright
  - Unsolicited commercial or advertising material
- Intentionally providing or submitting false information
- Intentionally restricting network traffic with high bandwidth use
- Flooding forums and other services unnecessarily or with inappropriate content/material
- Editing or modifying any element of the VLE without permission
- Using others' passwords or log-in identities
- Deliberately introducing any virus, worm, Trojan horse or other harmful or nuisance programme or file, or deliberately circumventing any precautions taken by the School to prevent this from happening
- Using any service for commercial purposes or profit
- Using any service for political purposes
- Using any service inappropriately during class time
- Copying any code, software or content provided without permission
- Violating copyright laws, data protection laws and computer misuse laws

**Please read this document carefully. Only once it has been electronically accepted will access to the Internet be permitted. If any student violates these provisions, access to the Internet will be denied and the student will be subject to disciplinary action.** Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

## **Students' Code of Practice**

- I will only use the internet when supervised by a teacher or adult.
- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- I will never send anyone my picture without permission from my teacher/parents/carer.
- I will never give my password to anyone, even my best friend and I will log off when I have finished using the computer.
- I will never arrange to meet anyone in person without first agreeing it with my parents/teacher/carer and get them to come along to the first meeting.
- I will never hang around in an Internet chat room if someone says or writes something which makes me feel uncomfortable or worried, and I will always report it to a teacher or parent.
- I will never respond to unpleasant, suggestive or bullying e-mails or bulletin boards and I will always report it to a teacher or parent.
- I will not look for bad language or distasteful images while I'm online and I will report bad language or distasteful images to a teacher or parent if I come across them accidentally.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I know that my teacher and the Internet service provider will check the sites I have visited!
- I understand that I can access only sites and material relevant to my work in school and that I will not be able to use the Internet if I deliberately look at unsuitable material.
- I understand that I will not be able to use the Internet if I deliberately hack into the schools' or other systems.
- I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I know that the contents of my e-mail messages will be monitored by the school
- I may not download software from the Internet (including screen savers, games, video clips, audio clips, \*.exe files).
- I know that information on the Internet may not always be reliable and sources may need checking. Web sites may be sponsored by advertisers.
- I will not use e-mail to send or encourage material which is pornographic, illegal, offensive or annoying or invades another person's privacy

## Staff Guidelines

The school has provided computers for use by staff. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

### **Equipment**

- **Do not** install, attempt to install, or store programs of any type on the computers without permission.
- **Do not** damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- **Do not** use the computers for commercial purposes, e.g. buying or selling goods.
- **Do not** connect any non-school mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) without the prior permission of the Business Manager.
- **Do not** eat or drink near computer equipment.

### **Security & Privacy**

- **Do not** disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number or your school's name, or send them your picture.
- **Do not** use the computers in a way that harasses, harms, offends or insults others.
- Respect, and **do not** attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and memory sticks/devices are open to review by the School to ensure that users are using the system responsibly.

### **Internet**

- **Do not** access the Internet unless for school activities.
- **Do not** use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- **Do not** engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others.

### **Email**

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed.
- **Never** open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.

The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to the Business Manager.



## **Access**

In order to access non-timetabled ICT resources staff must contact RECEPTION by telephone or via email (kwall@blpmail.org.uk).

Although the Library is no longer a bookable space, staff can send small groups of students to use the books/laptops but they would need to check with the Librarian first.

## **VLE - Terms of Use**

When using the VLE and connecting services users must

- Respect the rights of others.
- Remember to logout at the end of each session.
- Comply with current and future legislation including:
  - The Data Protection Act 1998
  - Copyright, Designs and Patents Act 1988
  - Telecommunications Act 1984
  - Protection from Harassment Act 1997

The following are not permitted at any time

- The creation, display, production, storage, circulation or transmission of pornographic or other offensive material in any form or medium (including sending, posting or displaying offensive images, language or any other type of offensive content including the bullying, harassment and intimidation of others.
- Users must not create, store or transmit:
  - Defamatory or libelous material
  - Material that infringes copyright
  - Unsolicited commercial or advertising material
- Intentionally providing or submitting false information
- Intentionally restricting network traffic with high bandwidth use
- Flooding forums and other services unnecessarily or with inappropriate content/material
- Editing or modifying any element of the VLE without permission
- Using others' passwords or log-in identities
- Deliberately introducing any virus, worm, Trojan horse or other harmful or nuisance programme or file, or deliberately circumventing any precautions taken by the School to prevent this from happening
- Using any service for commercial purposes or profit
- Using any service for political purposes
- Using any service inappropriately during class time
- Copying any code, software or content provided without permission
- Violating copyright laws, data protection laws and computer misuse laws

Please read this document carefully. Only once it has been electronically accepted will access to the Internet be permitted. If any staff member violates these provisions, access to the Internet will be denied and the staff member will be subject to disciplinary action.

## **Staff Code of Practice**

- Staff should be familiar with the school's Computer Resources Policy.
- Staff should closely monitor and scrutinise what their students are accessing on the

internet including checking the history of pages.

- Computer monitor screens should be readily visible for staff, so they can monitor what the students are accessing.
- Staff should make students clearly aware of the guidelines for the content of e-mail messages, as well as sending and receiving procedures.
- Use of the Internet should be monitored by Staff.
- Students should be taught skills and techniques to enable efficient and effective use of the Internet.
- Staff and Students should have a clearly defined focus for using the Internet and e-mail.
- If offensive materials are found the monitor should be switched off, any printed materials or memory devices should be confiscated and offensive URLs should be given to the Business Manager who will report it to the school's internet service provider.
- Virus protection has been provided by the school as viruses can be down loaded accidentally from the Internet. Staff and students bringing work from home, on memory devices, could also infect the computer - some viruses will format your hard disc.
- The school's internet service provider will check sites visited by schools.
- It is recommended that staff and students do not use open forums such as newsgroups or chat rooms.
- Disciplinary action may be taken if the Internet is used inappropriately e.g. for accessing pornographic, racist or offensive material for personal financial gain, gambling, political purposes or advertising.
- Software should not be downloaded from the Internet (including screen savers, games, video clips, audio clips, \*.exe files).

I have read the Computer Resources Policy Staff Guidelines and Staff Code of Practice and I agree to abide by these documents.

## **Review**

This policy will be reviewed in 4 years (earlier if any legislative change).

September 2015