PORTSMOUTH ENGLISH LANGUAGE SCHOOL

# Computer and Internet Acceptable Use Policy

## Introduction

The school provides computers for use by students and teachers. They offer access to a vast amount of information for use in studies. This policy applies to staff and students.

The computers are provided and maintained for the benefit of all staff and students, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Students are as responsible for good behaviour on the Internet as they are in a classroom. Inappropriate use of the internet will result in that privilege being taken away.

## 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 open files brought in on removable media (such as CDs, USB drives etc.) until they have been checked with antivirus software, and been found to be free of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be free of viruses.
- 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, 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.

## Internet

- The Internet should only be used for study or for school authorised/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 via the Internet. People you contact online are not always who they seem.
- Refer to our E-safety Policy for further details

**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 could destroy information and software on the computers.
- The sending or receiving of emails 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.

**Enforcement**

This document is to be read carefully by all staff and students. A copy will be issued to each staff member and a simplified version to each student, and this must be signed and returned to the school. If any student or staff member violates these provisions, access to the Internet will be denied and disciplinary action will be taken. Where appropriate, the police may be involved, or other legal action taken.

For students, 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.

**Risks**

The Byron Review (Safer Children in a Digital World 2008) classified the risks as relating to content, contact and conduct. The risk is often determined by behaviours rather than the technology itself.

- Commercial
- Aggressive
- Sexual
- Values
- Content (child as recipient)
- Adverts, spam, sponsorship
- Personal Information
- Violent/hateful content
- Pornographic or unwelcome sexual content
- Bias, racist and/or misleading information/advice
- Contact (child as participant)

- Tracking
- Harvesting personal information
- Being bullied, harassed or stalked
- Meeting strangers
- Being groomed
- Self-harm
- Unwelcome persuasions
- Conduct (child as actor)
- Illegal downloading
- Hacking
- Gambling
- Financial scams
- Terrorism
- Bullying or harassing one another
- Creating and uploading inappropriate material
- Providing misleading information/advice

**Principles for acceptable use of the Internet**

Staff are only permitted to use the Internet for personal use (this includes email) outside of their normal working hours (use is permitted during staff break and lunchtimes). Online activities which are encouraged include:

- The use of email for communication: between colleagues, between students(s) and teacher(s), between student(s) and student(s), between schools and industry.
- Use of the Internet to investigate and research school projects or topics related to social and personal development.
- The development of students' competence in ICT skills and their general research skills.

Online and other activities which are not permitted include:

- Copying, saving or redistributing copyright-protected material, without approval.
- Subscribing to any services or ordering goods or services, unless specifically approved by the school.
- Playing computer games or using other interactive 'chat' or 'social' sites unless specifically approved by the school.
- Using the network in such a way that use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages).
- Publishing, sharing or distributing any personal information about a user (such as: home address; email address; phone number; etc).
- Downloading software.
- Taking and storing images of children using mobile phones.
- Any activity that violates a school rule.

The school will:

- Use a firewall to filter and monitor access.
- Ensure virus and anti-malware protection is installed and updated regularly.
- Regularly discuss acceptable use with children and remind them of the school's policy and rules (this will include acceptable use of texting).
- Support parents in safe use of the Internet and other technologies.
- Ask parents to give consent for their children to use the Internet.
- Ensure teachers guide students toward appropriate materials on the Internet.
- Appoint a Designated Safeguarding Lead with responsibility for child protection/safeguarding.
- Ensure only those people with authorised access can access the school's IT network.

Children will:

- Have equal access to school-controlled email in a safe and secure environment.
- Have equal access to a variety of approved websites via the Internet.
- Be taught all the skills in order to use Internet and email as an ICT tool.
- Know how to report any concerns they may have.
- Use Internet and email to support, enhance and develop all aspects of the syllabus.
- Develop Internet and email skills at the appropriate level regardless of race, gender, intellect and emotional or physical difficulties.

Staff will:

- Ensure they keep data safe and secure.
- Conduct themselves professionally online; they must not allow children access to their own data through social networking sites such as Facebook; teachers are advised to block children from their class and school.
- Inform the Designated Safeguarding Lead of any issues of concern.

**Useful Websites**

- www.teachernet.gov.uk
- www.thinkuknow.co.uk/teachers
- www.childnet.com
- www.kidsmart.org.uk
- www.ceop.gov.uk/reportabuse/index.asp
- www.everychildmatters.gov.uk
- www.nen.gov.uk/hot_topic

This policy was created in June 2015 and reviewed in October 2015 by V Fortune. It is subject to review in April 2016 by the Designated Safeguarding Lead. The policy was reviewed in June 2016 by V Fortune and is subject to be reviewed again in October 2016 by the DSL.

PORTSMOUTH ENGLISH LANGUAGE SCHOOL

This policy was reviewed in October 2016 by Victoria Fortune, and it is subject to review in June 2017 by the DSL.

I have read and agree to the Computer and Internet Acceptable Use Policy and the e-safety policy.

Signed _____

Name_____

Position_____

Date_____