Acceptable Use Policy (AUP) of the ICT Network, Internet and E-mail

1. Aims of the Acceptable Use Policy (AUP).

The following is the schools policy governing the acceptable use of all computer equipment, including that of the Internet and E-mail. The main objective of the document is to highlight the '*personal responsibility*' of computer users at the school, whether for creating coursework, homework or browsing the Internet.

2. General Computer Use.

The following are guidelines that set out the acceptable use of equipment and use of computers generally around the school. This is to provide an environment where computers are accessible to staff and students alike, when needed. First priority must always be to ICT lessons and other planned lessons.

- **Passwords.**
  Passwords are the responsibility of the user and under no circumstances should they be disclosed in any way. Auditing software is used on the network to track usage by username: therefore if a username and password have been used it will be assumed to have been used by the owner. Passwords should be changed regularly and should be a minimum of six characters, preferably using letters and numbers. If you suspect that someone knows your password, you should change it immediately by contacting ICT Support who can do this for you.

- **User Areas.**
  User areas are the responsibility of the user. Any user found to have used excessive space on the network may have their account disabled so that they can be informed of this and asked to delete any old and unwanted files. It is hoped that all users will keep their network space tidy and free of any old and unwanted files. Students are encouraged to save files to their Office 365 OneDrive, which has almost unlimited capacity to save storage space on the school servers. ICT Support will search the user areas regularly to see if there are any unsuitable files. Unsuitable files are executable (.exe) files, certain graphics files and anything else deemed to be inappropriate. Users will be informed and expected to remove the files or they will be removed by ICT Support.

- **Computer Damage.**
  Any computer damage should be reported to a member of staff or ICT Support immediately.

- **Compact Disc's & USB Pen Drives.**
  Virus protection is installed on all computers throughout the school and will be kept up to date. If a personal disc is suspected of having a virus, it should be scanned before any files are transferred to the school's network. Any help in doing this can be obtained from a member of staff or ICT Support.

- **Printing.**
  In order to reduce wasteful printing and in line with other recycling and green initiatives, all users are allocated printing credit at the beginning of each term. Once this credit has been used, the user will no longer be able to print unless further credit is purchased. Please tick the box on the attached form to show that you are aware of the printing allocation and you accept that extra printing credit must be purchased.

3. Use of the Internet and e-mail.

The school uses a filtered, broadband Internet service provider (ISP) for e-mail and Internet access, throughout the school. Students will be allowed to access the Internet to search for information and resources to enhance their learning within the school. However, students need to be aware that anyone can publish material on the Internet. Some of this material can contain the opinions of others, bias or the information may not be valid. Students should try to validate material through cross referencing before use in school work. All material obtained from the Internet and included in school work should be clearly referenced. Students are not permitted to send e-mail internally throughout the school and any e-mail that is sent externally is automatically checked for certain words. Any e-mail found to contain these words is immediately filtered and sent to ICT Support, who will inform the Head of ICT.

The following forms a code of conduct that the school expects all users to adhere to:

- All users must obtain permission to use the Internet from their parent(s) before they will be allowed to access the Internet. Forms for this purpose should be sent out to all new students. If not they can be obtained from ICT Support.

- Any work or activity on the Internet must be related to school work.
- Use of the Internet for private means is prohibited.
- Use of the Internet for Facebook or other social media is prohibited at school and should be closely monitored at home by parents.
- Do not disclose to anyone, any passwords or login name that you have been given.
- Do not disclose any private details, including addresses, telephone numbers (mobile and land line) of yourself or anyone connected to the school.
- No games are to be played on the network, unless you are permitted to do so by a member of staff.
- Do not download, upload or use any material that is or may be under copyright. If in doubt ask a member of staff for guidance.
- Under no circumstances should you download, upload or view any material that may be unsuitable for children or schools. This applies to any material of a violent, dangerous, racist or inappropriate content.
- Use of Internet chat rooms is forbidden.
- Use of web based e-mail, such as Hotmail is forbidden.
- Any work that is to be sent from home to school via e-mail, should be sent to your schools e-mail address. I.e. username@burgate.hants.sch.uk
- All Internet usage in school will be monitored regularly and any inappropriate websites will be filtered via the schools built-in filtering and the school will inform the ISP, if outside filtering is required.
- Any user discovering unsuitable material in the Internet, should immediately inform their teacher or ICT Support. The websites URL (www.) address should be written down for filtering.

4. Consequences.

Failure to adhere to these conditions will result in:

a) Access to the Internet being removed. OR

b) User account being fully disabled. The duration of both actions above will be decided by the relevant Head of Year at the time of the offence. All users must also agree to their area on the network being searched for any content that could be dangerous to the network's security or inappropriate in any way and to being shadowed (watched) remotely whilst working.

5. Personal Laptops/Notebooks.

Any personal laptops/tablets that are brought in to the school should be sanctioned for use by the Head of Year and only used for school work. Users should also be aware of the following:

1. Connection to the school network is at the discretion of ICT Support and any configuration should only be done by ICT Support. This work will not be able to take priority.
2. If permitted on to the school network the computer should contain up to date Anti-Virus protection. ICT Support can advise if required.
3. The school cannot be held responsible for the security of personal laptops.
4. All personal laptops/notebooks will not be covered by the schools insurance, so separate cover would be required and is the responsibility of the owner.

Disclaimer.

The school will supervise students and take all reasonable precautions to ensure that users access only appropriate material, whilst in school. The school will provide a filtered Internet service. However, no system can be completely effective and a combination of approaches will be required to supervise adequately. As a result of the process involved in publishing information on the Internet, it is not possible to guarantee that unsuitable material will never appear on a computer screen. The school cannot accept liability for the materials accessed, or any consequences thereof.

If you do not understand any part of this Acceptable Use Policy, please contact the Head of ICT or ICT Support.