ACCEPTABLE COMPUTER USE POLICY

1.0   INTRODUCTION

1.1   The purpose of this policy is to ensure that staff and students understand the way in which the Internet, email and computers should be used at King Alfred School. The aim is to enable all staff and students including those children in the EYFS to gain maximum value from these facilities, to advise them of the dangers that can arise to themselves or the School if the technology is misused, and to advise staff and pupils of the consequences of misuse.

2.0   USE OF COMPUTERS IN SCHOOL

2.1   The provision of computers and associated technology is to support the education of students and to assist staff in the management of the school. To enable this:

2.1.2 Priority in the use of computer rooms during lesson time will be for the conduct of timetabled lessons. However other students may use the rooms with the permission of ICT teachers or other ICT staff.

2.1.3 The school operates an "open policy" which means that students can use the computer rooms without staff supervision. This policy relies upon students exercising a high degree of personal responsibility. Computer rooms are at times open during break times and before and after school provided a member of the ICT department has agreed this.

2.1.4 All computer equipment should be treated with care and staff and students should not alter the hardware configuration without the advice of a member of the ICT staff.

2.1.5 Neither food nor drink is allowed in the computer rooms. However, bottles of water may be taken in provided that they are used away from equipment.

2.1.6 Bags brought into the computer rooms are a safety hazard and should only be left under the central table. Where possible, bags should not be brought in at all.

2.1.7 Any Administrative computers may not be used by students. Students may not enter the IT office unless accompanied by a member of staff.

2.1.8 No attempt should be made to disable or compromise the security of information contained in the School's or other computers.

3.0   USE OF THE INTERNET

3.1   Access to the internet is provided in the school as an educational, administrative and management tool. All users are expected to use the facility responsibly and with regard to the needs and wishes of others.

3.2   Unsuitable sites (for example, those containing offensive, obscene or indecent material) will be blocked where possible and students and staff should not attempt to bypass these restrictions. If an unsuitable site is reached by accident then this should be reported to the ICT staff, the Head, a Deputy Head or the Bursar. Senior students may be granted access to particular blocked sites when this is requested by their subject teacher. Similarly staff may request the Head of ICT to allow access to a blocked site. Securus e-safety, and Smooth wall appliances are amongst some of the monitoring systems used to protect students and staff online. Please also see point 7.1.

3.3   Access to the internet within school may not be used for financial gain, gambling, political purposes or advertising, unless permission has been granted by the Head or the Bursar. The Internet should never be used to engage in computer hacking.

3.4   Students should never communicate any personal details (e.g. names, telephone numbers, home addresses) about themselves, or others, whilst using the internet except for university and other online college applications.

3.5   The use of web-hosted email accounts such as Hotmail is currently allowed but these must be used responsibly and without giving offence to others.

3.6   The downloading and deliberate accessing of offensive, obscene or indecent material or material containing a virus is not allowed. If this occurs it will be reported to the Head and (if done by a pupil) to Parents, for appropriate action to be taken. Students are taught how to be safe online and what measures the school takes to help keep them safe in school, during ICT lessons, Form Hour and PSHE lessons.

3.7   Students and staff should be aware that whilst the Internet provides enormous opportunities for research, some information may be less accurate than it may appear. Senior students should take advice from their teachers about validating information obtained from the Internet.

3.8   Pupils must not commit the School to any form of contract through the internet without the express permission of a teacher. Staff may only enter into a contract on behalf of the School through the internet in connection with the proper performance of their duties.

4.0   USE OF EMAIL

4.1   Staff and students may use email for educational, school business and personal purposes, but they are expected to use it responsibly. This facility may be denied if a person uses it excessively for personal use, in a manner which could cause offence or distress to others, or in a way which compromises the day to day business of the school. The sending of offensive email will not be tolerated (see paragraph 7.1).

4.2   Users of the system should think carefully before sending or forwarding emails. If a student or member of staff receives an email clearly intended for another person they should inform the sender and redirect the email to the correct person. They must not use any information contained in the email nor tell anyone else about its contents, but they should immediately tell a member of the ICT staff what has happened.

5.0   COPYRIGHT ISSUES

5.1   Generally, software purchased under licence cannot be given to students to install on personal computers. However there are certain applications which we are allowed to share and students will be offered these where applicable.

5.2   Students and staff should not download software without the consent of either IT staff or the Bursar. Whilst firewalls and other precautions are in place, the School's systems are vulnerable to damage by viruses and these are prevalent in downloaded programs and executable files. It is illegal to knowingly spread viruses.

5.3   Students and staff must not attempt to interfere with or alter settings on any school computer or seek to attain access to restricted areas without the consent of a member of the IT staff or the Bursar. Disciplinary procedures may be invoked if appropriate.   Unauthorised access to or modification of computer material may leave perpetrators open to prosecution under the Computer Misuse Act 1990.

5.4   Information obtained from internet sources will generally belong to a person or organisation and may have copyright restrictions. Such information, including text, graphics, sounds and moving images may not be published outside the school in any form. However the law permits that **this information may be used in internal publications or,**

specifically, for examination coursework. Where such information is used ownership must be acknowledged in a bibliography.

5.5   Everyone, but especially examination candidates, should be aware that information obtained from the Internet, or other sources, cannot be passed off as one's own work.

6.0   CONNECTION TO THE SCHOOL NETWORK

6.1   Students and staff may only connect to the school network using their own logon name and password. You should keep your password secret and not disclose to anyone else. If you believe that someone knows your password, either change it or seek the assistance of ICT staff to change it.

6.2   Designated systems administrators may use system passwords when carrying out their duties as administrators.

7.0   MONITORING

7.1   In the rare cases where the School has reason to believe that a student or member of staff has been misusing the School's computer network, Internet or email, it may monitor that person's use of these facilities. However, the school will normally respect the privacy of an email if it is clearly marked as personal, unless the School honestly believes that there are good reasons to examine its contents. Students and staff must be made aware that the school's software does screen for inappropriate usage and the School has the right to investigate and to follow up any issues.