ACCEPTABLE USE OF ICT (INFORMATION & COMMUNICATION TECHNOLOGIES) & SOCIAL MEDIA POLICY

This policy was adopted on:	27.11.13
Policy last reviewed on:	10.01.21
Person/Body reviewing:	DSL/Heads of Digital Learning/Executive Board
Date of next review (except in the case of relevant legislation):	10.01.22
Published:	ISI/Governors/Staff/Pupils/Website

Introduction

The following pages comprise the complete Policy document covering acceptable use of the school's computer systems, the Internet and associated media by pupils and staff. It is assumed that all staff have read and agreed the contents of this policy and the 'Rules' governing responsible use of the school's computing facilities and Internet access/ usage by pupils and staff. These 'Rules' have been developed in response to recommendations from Kent County Council, the DfE and other appropriate agencies.

All parents and pupils are informed of the content of the policy and parents are asked to sign an e-safety agreement (in Appendix 1), agreeing to their/ their child's compliance with school 'acceptable use' procedures

Internet Acceptable Use

The Internet is as commonplace as the telephone or TV and its effective use is an essential life-skill. However, unmediated Internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. A policy is required to help to ensure responsible use and the safety of pupils.

The purpose of Internet use in the school is to support learning, raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's public image, management of information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The Internet is an essential element in 21st Century life for education, business and social interaction and the school aims to provide pupils with quality Internet access as part of their learning experience.

Benefits of Using the Internet in Education include:

- access to world-wide educational resources such as museums and art galleries;
- access to teaching and learning webtools such as Seesaw and Google Classroom;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and systems;
- exchange of curriculum and administration data;
- enhancing the visibility of the school, its achievements and provision to both existing and prospective parents.

Internet Use to Enhance Learning

- The school Internet access will be designed expressly for staff and pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.
- Excessive personal use of the Internet is unacceptable and should never interfere with teaching and learning, or with the efficient discharge of staff duties.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval together with the correct identification of ownership and Copyright.
- Where digital classrooms (such as through Seesaw or Google Classroom) are created for the purpose of providing pupils with the ability to electronically exchange commentary and/or information relevant to a particular topic, these will be considered as a virtual extension of the classroom, and all King's Rochester rules and regulations will apply.

Pupils' Evaluation of Internet Content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Services Manager. (Pupils will normally report such sites to their teacher at the time.)
- The use of Internet derived materials by staff and by pupils must comply with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to judge the validity of information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

The Management of Email

- Pupils may only use their approved, school email accounts on the school system. Access in school to external personal email accounts is forbidden.
- Pupils must immediately tell a teacher if they receive offensive spam/non-school related email.
- Pupils must not reveal details of themselves or others, such as passwords, address or telephone number, or arrange to meet anyone in email communication.
- All pupils and staff will be allocated a school email address when they join the school. Pupils and their parents will be required to sign a form to confirm their agreement to the school email and Internet usage policy. (See Appendix 1).
- Excessive personal use of email is unacceptable and should never interfere with teaching and learning, or with the efficient discharge of staff duties.
- Emails sent to an external organisation should be written carefully and in the same way as a posted letter.
- The forwarding of chain letter emails is banned.
- Staff should only use regulated/monitored school email accounts to communicate with pupils, parents or professional business contacts.

The Management of Web Site & Digital Learning Platforms

- The school has a website for public dissemination of information, the content of which is overseen by the school's Director of Marketing, the Principal and Headteachers.
- The school uses SeeSaw and Google Workspace with its related online tools, in particular Google Classroom, to communicate teaching and learning material with pupils, and were appropriate, parents. The service is overseen by the Heads of Digital Learning and the Computing Subject Lead in each section of the school.
- In the case of Google Classroom, a digital service called Salamander Soft, maintains a direct, daily synchronised link between ISAMS and Google Classroom, creating all digital classes and populating them with pupils as allocated in ISAMS. Each Google Classroom class has teachers and pupils allocated to them. A quality assurance account for each year group is also added for quality assurances purposes, the log-in details of which are shared with the Heads of Digital Learning, ISAMS co-ordinators and relevant Senior Management staff.

- No staff member will be permitted to rename or create extra classes without permission from the Heads of Digital Learning and the Computing Subject Lead in his/her section of the school. Any staff member managing a class within the Google Classroom/SeeSaw sites, will be asked to be responsible for appropriate content/ discussion threads linked to current classroom topics.
- Any staff or pupils misuse must be reported to the Principal/Headmaster of the Preparatory School/Headmistress of the Pre-Preparatory School/Heads of Digital Learning Computing Subject Lead immediately; teachers are responsible for ensuring that all posts are checked and excluded if they include examples of inappropriate language, plagiarism, personal data which makes the child overtly identifiable (such as, but not limited to: surname, email address, phone number or discreet school information), information not relevant to classroom discussions, threats or discriminatory comments, Copyrighted information, solicitations or advertisements of any kind.
- The point of contact on the school's Web site and/or Classroom pages will be the school address, school email and telephone number or official staff email contact details. Staff or pupils' personal/ home information will not be published.
- Publishing images, videos or audio clips of pupils on the school's website or Classroom pages or other educationally-linked web pages can be highly motivating and encouraging. However Data Protection issues must be considered when publishing any such material on the Internet. Digital images, audio or video clips of school events or of school pupils taken by school staff and pupils will usually be taken using school equipment and digital files stored safely on the school's computer network, accessible only to staff (and/or pupils, where appropriate) prior to upload to the school's websites.
- If images or videos of pupils are published on the school website or school-linked websites, the Data Protection Acts (1988 and 2003) apply. To avoid images published online being edited inappropriately or misused, group photos and projects will be published on the website, in promotional material or online whenever possible, rather than full-face photos/ videos of individual children. Content focusing on individual pupils will not be published on the school website without parental permission.
- The use of names for any children appearing in photographs on our website or blog sites, or in any other media where it is necessary to name a child, will be limited to first names only, except in instances agreed with parents in advance. Videos will be at low resolution and password-locked, as appropriate and parental permission will always be sought prior to use of photographs/videos of individual children being used for promotional purposes. Personal pupil information including home address and contact details will not feature on web or blog pages. The school will ensure that published image files are appropriately named and will not use pupils' names in image file names or ALT tags.
- Pupils may be given the opportunity in some classes to publish projects, artwork or school work on the Internet in educationally recognised sites, or onto the school's website or Classroom pages. Web pages will be checked to ensure that there is no content that compromises the safety of pupils or staff and the publication of pupil work or images will be overseen by a supervising teacher in each section of the school. Pupils' work will always appear in an educational context on Web pages.
- The Director of External Relations, acting as the Principal's nominee, will take overall editorial responsibility for published material and ensure content is accurate and appropriate. Any concerns regarding any published material must be reported straightaway to the Director of External Relations.
- Any material which is sensitive should be password-protected or ideally published in an alternative manner directly to those who need to view it.

The copyright of all material will be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Management of Social Media

Introduction

The school acknowledges that the Internet provides a range of social media tools which allow users to interact with one another. These include discussion groups and newsgroups, social networking facilities such as Twitter, Facebook, Instagram, WeChat, YouTube and messaging–based media, and online, collaboratively-edited, internet-based documents such as Wikipedia. All use of emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is permitted. Staff and pupils are reminded that any post/ 'tweet' or message may not remain private and that their post will represent them as a member of the King's Rochester community. Therefore no staff member or pupil should engage in activities involving social media which might bring King's Rochester into disrepute.

Purpose

This policy applies to the use of social media for school and personal purposes, whether during normal, working hours or in your personal time. Its purpose is to help staff and pupils to avoid the potential pitfalls of sharing information on social media sites and should be read in conjunction with the School's Acceptable Use Policy.

IT facilities

The policy applies regardless of whether the social media is accessed using the School's IT facilities or on personal equipment.

- The school permits the incidental use of the internet and social media as long as it is kept to a minimum and takes place substantially outside normal working hours for staff and outside school hours for pupils. Use must not interfere with staff's work commitments or pupils' study commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Principal.

Guiding principles

Staff and pupils are required to behave responsibly at all times and to adhere to the following principles:

- Pupils should not identify themselves as pupils of King's Rochester in their personal web use and should ensure their private communications are set to appropriate privacy levels.

- Staff and pupils should always make clear that internet posts represent their own views and must not allude to other people's personal views in internet posts.

- Staff are prohibited from accessing social media from School computers at any time unless for official School business. Neither should social media be accessed by staff from a personal laptop or mobile phone device during School hours.

- Staff should not be 'friends' with current pupils or those who have left within the past two years on any social media network and it would be considered inappropriate to add current pupils or any pupil who has left within the past two years as 'friends' on a personal account. It may also, depending upon the circumstances, be inappropriate to add parents, guardians or carers as 'friends'. If in doubt, in the first instance, staff should bring their concerns to the attention of a Deputy Head in each part of the school who will advise.

- School-based tweeting will take place only using a Twitter account, set up and managed by authorized staff in school, and overseen by the Director of External Relations. Passwords will only be released to members of staff when the senior leadership team, the ICT Services Manager and Heads of Digital Learning and Computer Subject Lead are agreeable.

- Pupils 'tweeting' in school will use a classroom account, and never a personal account. They will be identifiable only by initials.

- Pupils and staff with personal Twitter accounts should protect their tweets to ensure that their Twitter feeds remain invisible to all but their own followers and to ensure that their private and School lives remain separate.

- Administrators of King's Rochester Twitter accounts will make informed decisions on a case by case basis to block followers based on their available biography and content: any followers with inappropriate messages or images in their feeds will be blocked and will be reported to Twitter if abusive or defamatory. King's Twitter accounts will only actively seek to follow others where following an '@ handle' has obvious benefits for the school.

- Pupils and staff should familiarise themselves with the privacy settings of any social media they use and ensure that public access is restricted. If they are not clear about how to restrict access, then all information posted should be regarded as publicly available and should therefore be edited accordingly.

- No posts should be made which may offend, insult or humiliate others, particularly on the basis of their sex, age, race, colour, national origin, religion or belief, sexual orientation, disability, marital status, pregnancy or maternity.

- No posts should be made which could be interpreted as threatening, intimidating or abusive. Offensive posts could be construed as cyber-bullying.

- Staff and pupils must be mindful of how they present themselves and the School on social media. Both are entitled to a social life like anyone else but extra-curricular lives have consequences which must be considered at all times when sharing professional information.

- When writing an internet post, it is wise to consider whether the contents would be more appropriate in a private message. Even if staff and pupils have strict privacy controls in place, information can still be shared by others. It is sensible to assume that any information posted will not remain private.

- Personal information such as names, addresses, email addresses, home or work addresses, phone numbers or other personal information should not be posted so that your privacy and that of others is protected.

- Staff who have a web-presence on professional business sites such as Linkedin where it is essential to provide personal details such as Job Title, Place of Work etc should be aware that these are also visible to a wider public and represent themselves accordingly, especially when joining a Group or Discussion Forum.

- Disparaging or derogatory remarks about the School, pupils or any of its staff or Governors, pupils, guardians or carers must not be posted.

- Staff members must not have contact through any personal social medium with any current pupil or any pupil who has left the school within the past two years, unless the pupils are family members, or with pupils' family members if that contact is likely to constitute a conflict of interest.

- Photographs, videos or any other types of images of pupils and their families, or images depicting staff members wearing school clothing bearing school logos or which identify sensitive school premises such as Boarding Houses must not be published on personal web space.

- School logos should not be used on personal web space or posted without the knowledge of the school's Executive Board.

- Staff should not access and edit online encyclopaedias in a personal capacity at work (e.g. Wikipedia) as the source of the correction will appear as the school IP address.

- Pupils and staff may only use official school-approved sites to communicate with pupils or to enable pupils to communicate with one another e.g. email/ approved school classroom pages.

- Pupils will not be allowed access to public or unregulated discussion/ messaging forums and members of staff are discouraged from accessing these within the workplace.

- Pupils may use only regulated educational messaging environments. This use will always be supervised and the importance of purposeful discussion and e-safety emphasized.

Social Media will not be made available unless an educational requirement for their use has been demonstrated.

The Use of Mobile Phones and other Personal Mobile Devices

- At King's Rochester, it is accepted that mobile technologies can enhance the curriculum for pupils and provide an instant and easily accessible method for staff to access planning, projects, the school management system, assessments and documents. The school's wi-fi network is available to pupils and staff for educational purposes. It is also recognized however that when used inappropriately, mobile technologies can offer distraction from teaching and learning, and create a negative impact on the learning environment for children. In extreme cases, the presence of mobile technologies can also impact negatively on the safety of pupils. Guidance about conduct and safe practice, including safe use of mobile phones by staff and volunteers, will be given at induction and included in all staff handbooks to ensure their personal safety and that of children in our school.

- Mobile phones and other personal mobile devices should not be used during lessons or formal school time, unless they provide a benefit to the pupils' education, or are required to communicate during an emergency.

- In the EYFS, no personal mobile phones or tablets are to be in used at any time when pupils are present, or to be in sight of pupils at any time. They should be kept in the school or Nursery office or in a locked cupboard. School devices are provided for use in the EYFS.

- Google Meet, Zoom or video-conferencing facilities may be used by pupils for educational use under staff supervision only.

- Senior managers and teachers may make use of all of the above media for educational/ business purposes as long as a clear rationale for their use has been identified e.g. interviewing an overseas pupil by remote access due to distance.

- Staff members will not use personal mobile phones to telephone or text message pupils directly. Contact with pupils should be via a regulated school email account or accepted educational social media environment. E.g. Google Classroom or SeeSaw.

Authorisation of Internet Access

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up to date, for instance when a member of staff leaves or a pupil is withdrawn.

- Pupils in Upper 6th will have their accounts locked down by the end of August in their school year. Pupils in other year groups will have their accounts locked down within 24 hours after leaving the school.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Pupils (parents in the case of Pre-Preparatory School pupils) will be asked to sign and return an e-safety form (see Appendix 1) on entry to the school, which authorises them to use the internet safely in school.
- In addition, regular e-safety awareness sessions will be carried out for all pupils each academic year to ensure pupils maintain an overview of current school e-safety policy.

Risk Assessment

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for children or for certain age-groups. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Any material that the school believes is illegal or puts children at risk, must be reported to appropriate agencies such as CEOP (Child Exploitation and Online Protection Centre) in line with the Safeguarding and Child Protection policy and also to the Designated Safeguarding Lead.
- The Principal and Executive Board will ensure that this 'Acceptable Use of I.C.T. Policy' is implemented and compliance with the policy monitored. Heads of Digital Learning and the Computing Subject Lead will play an integral role in this process.
- The school will make every effort to inform parents if their child has inadvertently or purposefully viewed inappropriate material.

The Management of Filtering

- The school will work in partnership with parents, Smoothwall (the relevant filtering software agent) and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved annually.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported either directly to the ICT Services Manager, or to Heads of Digital Learning or Computing Subject Lead.
- Any material that the school believes is illegal must be referred to CEOP.
- A filtering software (Smoothwall) will be utilized by the school to filter and monitor pupil and staff usage of the internet and alert the school to safeguarding issues through inappropriate usage. It is the responsibility of the IT team to report timeously to the designated safeguarding lead (DSL), Mrs Catherine Openshaw, Headmistress of the Pre-Preparatory School, any misuse of the school's system, e.g., cyber-bullying, or pupils making searches relating to extremism. Any misuse will be dealt with in accordance with the school's disciplinary and safeguarding policies.
- If a member of staff is concerned that a pupil of the school is a victim of radicalization or is spreading radical views, the Prevent referral form V15/08/2012 may be used to report a concern and emailed to channel@kent.pnn.police.uk This form can be completed by any concerned adult, but will usually be completed by the DSL or one of her deputies. If it is completed by someone else, then the DSL needs to be informed at the earliest possible opportunity. Alternatively, local Police can be contacted on the non-emergency number – 101.

The Introduction of Policy to Pupils

- Rules for Internet access and e-safety will be posted in common online areas accessible to all staff and pupils.

- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Consideration will be given to a module on responsible Internet use for inclusion in the PSHEE or Computing / EdTech programme, covering both school and home use, each academic year.

Staff Consultation

- All staff will be made aware of the School's 'Acceptable Use of ICT Policy' at the point of induction and via staff handbooks, and its importance explained. They will be asked to accept the terms of this policy before using any Internet resource or ICT equipment/ technologies in school and ongoing CPD will be planned and deployed across all three schools.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user.

Discretion and professional conduct are essential.

- In addition, staff will also be asked to sign the agreement.

The Maintenance of ICT System Security

- The school ICT systems will be reviewed regularly with regard to security.
- Antivirus and other Anti-Malware software will be installed and updated regularly.
- Security strategies will be discussed with service and support providers, particularly where a wide area network connection is being planned. External storage devices will be automatically scanned by Antivirus software.
- Files held on the school's network and on online platforms like Google Drive will be regularly checked.
- The downloading of unauthorised files, including executable that can compromise system performance is prohibited.
- The ICT Services Manager will endeavour to ensure that the system has the capacity to take increased traffic caused by Internet use after an annual review.

The Management and Storage of Personal Data

- The school's management information system (ISAMS), the pre-admissions system (RSAdmissions) and academic information system (PASS) necessarily contain a variety of data about pupils, families and staff, most importantly so that contact can be made in an emergency, teaching can be based upon assessment of learning, and communication can be maintained effectively with all parents connected to the school.
- King's Rochester takes care to manage such data responsibly, keep adequate but not excessive records, maintain and secure data carefully, and to meet its statutory obligations under the Data Protection Act 1998 and 2003. Any current or prospective member of the school community has a right to know what data is held about them. For further information, refer to the School's Data Protection Policy.

Archiving of Pupil and Staff Files

- In order to help furnish references, and in the event of query after a pupil or member of staff has left, King's stores pupil and employee files after pupils and staff have left the school.
- Hard copy paper files are scanned and stored to USB drive or secure online platforms like Google Drive. They are stored in a secure location under lock and key. Two sets are produced of each set of archived data and each disk/ drive is stored in a separate secure location. These files are stored on USB drives as PDFs are not encrypted.
- Only school employees with appropriate data access privileges are allowed access to the files. Paper copies of documents are safely destroyed or rendered illegible e.g. by shredding, once scanning has taken place.

The Handling of Complaints/ Breaches of Policy

Staff

- Responsibility for handling incidents regarding staff misuse of any ICT equipment or abuse of this policy

will be delegated to the Principal in line with the school's complaints/ staff whistle blowing procedures. Any breach of this policy may lead to disciplinary action being taken against the staff member in line with the school's disciplinary policy and procedures.

- Potential child protection issues must be referred to the Designated Safeguarding Lead. Advice on dealing with illegal use may be sought from the Local Authority Designated Officer and/or the Local Children's Safeguarding Board (Medway) or with CEOP team. As with drugs issues, there may be occasions when the police must be contacted. Early contact may be necessary to establish the legal position and discuss strategies.

Pupils

- Any misuse of computer network technologies, email, or the school computer network and infrastructure by pupils should be referred to the Heads of each school or to the Principal. In this instance, the Principal or Headteacher will deal with the matter in line with the School's disciplinary procedures. The Principal reserves the right to remove a child's privileges to access the Internet or school network and will inform parents and police if such measures are necessary.

The Detection and Management of Cyber Bullying

- Cyber bullying (along with all forms of bullying) will not be tolerated in school
- The school promotes awareness of cyber bullying via Digital Learning, CPSHE and PSHEE sessions appropriate to age in all three parts of the school.
- Any incidences of cyber bullying are dealt with as part of the school's anti-bullying policy and/or child protection procedures.
- Any concerns should be directed to a senior teacher in the appropriate section of school.

Enlisting Parents' Support

- Parents' attention will be drawn to the School's Acceptable Use of ICT Policy at the point of registration and in school literature as appropriate.
- Internet issues will be handled sensitively to inform parents without undue alarm as stated above.
- Relevant leaflets from/ presentations by and links to e-safety organisations will be distributed whenever these are available to parents and pupils.

Appendix 1

E-Safety and Acceptable Use of ICT Agreement

The essence of this agreement is to encourage respect for all ICT users and safe use of the School's computer networks and equipment. The 'E-Safety and Acceptable Use of ICT Agreement' has been developed using national guidelines, as an essential part of the School's 'Acceptable Use of ICT & Social Media Policy'.

This form comprises part of each child's records as they move forwards in the school and, although some of the statements may not be relevant at early stages of a child's academic career, will apply as they develop their ICT skills. By signing this form, pupils are pledging to ensure, as far as is possible, that they will adhere to the requirements of this code of conduct, and staff sign to agree to adhere to the policy of the school.

(We ask that parents/guardians please speak with younger children about their responsibility concerning the use of technology within school, and sign on behalf of their child in the Pre-Preparatory School.)

This policy is set out to ensure that all computer users are aware of how to use the computer network and Internet appropriately. In this way, they should not have access to view or do anything unsuitable, damaging to other users' work, damaging to the network, or illegal.

You are asked to sign this agreement to enable you to safely use the School's ICT and email facilities.

Use of the School Networks

I understand that I must not:

- Access or attempt to access other users' files;
- Use anyone else's username;
- Create messages or documents that appear to originate from someone else;
- Create/publish any document that may be considered to be abusive, cause distress or otherwise be a nuisance;
- Try to configure or change any settings on the School computers;
- Attempt to bypass or defeat any School Computer or Network security controls;

- Use or attempt to use the School Computers for any purpose other than school-related assignments/ tasks.

I agree to:

- Keep my passwords secret;
- Look after the equipment I use;
- Notify the ICT Services Manager of any suspected misuse of my user area.

Use of the Internet and Electronic materials

I agree NOT to:

- Look for, or view, any inappropriate material;
- Send abusive emails, messages or anything that might upset others;
- Use public or unregulated discussion/ messaging forums;
- Use the school's computer resources for anything other than school-related assignments and tasks;
- Use mobile phones during lessons or formal school times without permission.

Personal Use of Technology

The school acknowledges that the Internet provides a range of social media tools which allow users to interact with one another. These include discussion groups and newsgroups, social networking facilities and messaging–based media, and online, collaboratively-edited, internet-based documents such as Wikipedia.

All are reminded that any post, 'tweet' or message, by the very nature of the medium, cannot remain private and that their post will represent them as a member of the King's Rochester community. Therefore, no member of the school community should engage in activities involving social media which might bring King's Rochester into disrepute.

It is strongly inadvisable for any pupil under the age of 13 to open such an account and most UK social-networking sites do not permit this by law.

Older pupils should bear in mind that any accounts unprotected by passwords are on view to the general public - including those universities to which they may apply in the future as well as potential employers, all of whom now view such sites for prospective employees.

I agree

- To password protect my profile and comments on any such site.
- Not to write or post any images on any sites which may damage my own reputation or that of King's.

I accept that:

The ICT Services Manager has access to all files and internet searches; these may be accessed at any time; the use of the network and internet is also monitored; in exceptional circumstances, emails may be read on the instructions of the Principal, Headmaster or Headmistress or the ICT Services Manager.

In addition I accept responsibility for:

- Logging off a computer before leaving it;
- Saving my work regularly;
- Keeping adequate back-ups of work done on non-networked computers, particularly coursework.

Private Computers and Personal Mobile Devices in School

Particularly within the Preparatory School, Senior School and our Boarding community, there will be occasions when pupils are permitted to use their own computers, tablets or mobile phones in School. This should always be with parental consent.

However, if these devices are misused in any way, they may be confiscated. These devices are permitted to connect with the School network using the Wi-fi network only. In order to be protected, boarders must only connect to the network using the connections in their rooms or Wi-fi in the Boarding Houses.

Pupils are responsible for the safe-keeping and insurance of their own devices.

Incident Reporting

Pupils who require help or report incidents are advised to contact any member of staff or the Head of Digital Learning or Computing Subject Lead in their section of the school.

The school's disciplinary procedure will be followed in the event of any breach of this agreement.

PLEASE SIGN ONE COPY OF THIS FORM AND RETURN TO THE SCHOOL OFFICE.

PUPIL'S/ STAFF MEMBER'S NAME (Please print):.....

I have read and agree to abide by the above Policy

Signed..... (Pupil OR Parent/Guardian in Pre-Preparatory School OR Staff Member)

Date.....