E Safety Policy

Headteacher	**Sign and Date:**	Darren Ayling Mr Darren Ayling
Chair of Governing Body	**Sign and Date:**	Mr Kevin Palmer

Date for next review:	October 2019

Scope of the Policy

This policy applies to all members of The King's (The Cathedral) School community (including staff, pupils/students, volunteers, parents/carers, visitors, community users) who have access to and are users of the School ICT systems, both in and out of The King's (The Cathedral) School.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils/students when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the School, but is linked to membership of the School. The School will deal with such incidents within this policy and associated behaviour and anti-bullying and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of School.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils/students resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The School provides the necessary safeguards to help ensure that the School has done everything that could reasonably be expected to manage and reduce these risks. The E-safety Policy explains how the School intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communication technologies for educational, personal and recreational use.

It is essential that this policy is read and used in conjunction with other School policies to include, the ICT Acceptable Use Policy for School Staff, Students Acceptable Use of ICT Policy, Anti Bullying Policy, E Safety for Students Policy, Safeguarding and Child Protection Policy and Mobile Phone Policy.

Roles and Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the School.

Governors

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. Governors will receive regular information about e-safety incidents as part of the Child Protection agenda item at Full Governors.

Senior Leadership Team (SLT)

The SLT are responsible for ensuring:

- The safety (including e-safety) of all members of The King's (The Cathedral) School community.
- Adequate training is provided.
- Effective monitoring systems are set up.
- That relevant procedures in the event of an e-safety allegation are known and understood.
- Reviewing the e-safety policies and documents.
- The Schools Designated Child Protection Officers should be training in E-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT, and monitor the risk of radicalisation for both pupils/students and staff. They will ensure staff are trained and regularly updated on the PREVENT duty and will make necessary referrals about any concerns that are presented through the designated PREVENT lead.

Deputy Headteachers/Assistant Headteachers
The DHT's and AHT's take day to day responsible for e-safety issues and have a leading role in:

- Liaising with staff, the LA, ICT Technical Staff, Governors and SLT on all issues relating to e-safety.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff.
- Receiving reports of e-safety incidents, and review the E-safety education programme in School.

Information and Communications Manager /ICT Technicians
The Information and Communications Manager and ICT Technicians are responsible for ensuring that:

- The School's ICT infrastructure is secure and meets E-safety technical requirements.
- The School's policies with regards to passwords are adhered to, using the ICT Acceptable Use Policy for both staff and pupils/ students, and the e-safety for student's policy.
- The use of the Schools ICT infrastructure (network, remote access, e-mail, School gateway etc.,) is regularly monitored in order that any misuse or attempted misuse can be reported to SLT for investigation/action/ sanction.

Subject Leader for ICT

- Subject Leader for ICT keeps up to date with e-safety technical Information.

Teaching and Support Staff
Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current School e-safety policy and practices and the Schools ICT policies.
- They have read, understood and signed the ICT Acceptable Use Policy for School staff.
- E-safety issues are embedded in all aspects of the curriculum and other School activities.
- Pupils/Students understand and follow the School's e-safety and Acceptable Use of ICT Policies.
- Pupils/Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activities in lessons, extra-curricular and extended School activities.
- In lessons where the Internet use is pre-planned, pupils/students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Designated Person for Child Protection/Child Protection Officers
Should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate material.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Pupils/Students

- Are responsible for using the School ICT systems in accordance with the Students Acceptable Use of ICT Policy.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of School and realise that the School's e-safety Policy also covers their actions out of School, if related to their membership of the School.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues are less experienced in the use of ICT than their children. The School will therefore take every opportunity to help parents/carers understand these issues, through parent's evenings, letters and the Schools website. Parents and carers will be encouraged to support the School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at School events.
- Access to on-line pupil/student records.
- Their children's personal devices in the School (where this is allowed).

Education and Training

E-safety Education will be provided in the following ways:

- Pupils/Students are helped to understand the need for the Student Acceptable Use of ICT Policy and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of School.
- Pupils/Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in School.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- A planned e-safety programme is provided as part of the assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum, this programme covers both the use of ICT and new technologies in School and outside of School.

Copyright

- Pupils/Students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations, staff to monitor this.
- Pupils/Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images, staff/pupils/students should open the selected image and go to it's website to check for copyright.

Staff Training

- SLT will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- All new staff receive e-safety training as part of their induction programme, ensuring that they full understand the School E-safety policy, ICT Acceptable Use Policy and Safeguarding and Child Protection Policy.

Communication

This is an area of rapidly developing technologies and uses. The King's (The Cathedral) School consider the following as good practice when using communication technologies:

- The School email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils/students should therefore use only the School's email service to communicate with others when in School, or on the School's systems (e.g. by remote access).
- Digital communications with students (e-mail, online chat, School gateway etc.,) should be on a professional level and only carried out using official School systems (see staff guidance in Child Protection Policy and Staff Code of Conduct).
- Under no circumstances should staff contact pupils/students, parents/carers or conduct any School business using personal e-mail addresses.
- School e-mail is not to be used for personal use. Staff can use their own e-mail in School (before, after School and during lunchtimes when not working with pupils/students) - but not for contact with parents/students.
- Personal information should not be posted on the School's website and only official e-mail addresses should be used to identify members of staff.

Mobile Phones

- **School** mobile phones only should be used to contact parents/carers/pupils/students when on School business with pupils/students off site. Staff should not use personal mobile devices.
- **Staff** should not be using personal mobile phones in School during working hours when in contact with pupils/students.
- Pupils/students should adhere to the rules and guidelines set out in the Mobile Phone Policy.

Social Media/Networking Sites

Young people will not be allowed on social networking sites at School; at home it is the parental responsibility, but parents/carers should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on School equipment in School or at home. Staff should access sites using personal equipment.
- **Staff** users should not reveal names of staff, pupils/students, parents/carers or any other members of the School community on any social networking site or blog**.**
- **Pupils/students/parents/carers** should be aware the School will investigate misuse of social networking if it impacts on the wellbeing of other pupils/students/staff or stakeholders.
- If inappropriate comments are placed on social networking sites about the School or School staff then advice will be sought from the relevant agencies, including the police if necessary.
- Pupils/students in the KS3 curriculum will be taught about e-safety on social networking sites as we accept some may use it outside of School.

Although many of the above points are preventative and safeguarding measures, it should be noted that the School will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The School has an active website and twitter account which are used to inform, publicise School events and celebrate and share the achievement of pupils/students.

Digital/Photographic Images

- The School record of parental permissions granted/not granted must be adhered to when taking images of our pupils/students, a list can be obtained from the SIMS Administrator.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher.
- Where permission is granted the images should be transferred to School storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

Removable Data Storage Devices

- Only School provided removable media should be used
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards, etc.) must be checked for viruses using School provided anti-virus software before run, opened or copied/moved on to local/network hard disks
- Pupils/students should not bring their own removable data storage devices into School unless asked to do so by a member of staff.

Websites

- In lessons where Internet use is pre-planned, pupils/students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger pupils/students who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents/Carers** will be advised to supervise any further research.
- **All** users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which pupils/students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the pupils/students on the internet by the member of staff setting the task. All staff are aware that if they pass pupils/students working on the internet that they have a role in checking what is being viewed. Pupils/students are also aware that all internet use at School is tracked and logged.
- The School only allows SLT and the Network Manager to access to Internet logs.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file.
- Passwords should be changed at least every six months.
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems.

Students

- Inform staff immediately if passwords are traced or forgotten. All staff should contact our ICT Support Office to change passwords.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the School's network without the specific permission of the Headteacher or the Network Manager.
- Students should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to School ICT equipment.
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

All use of the School's Internet access is logged and the logs are randomly but regularly monitored by the School's Network Manager. Whenever any inappropriate use is detected it will be followed up by the Pupil Development Managers (PDM's) or members of the Senior Leadership Team, depending on the severity of the incident.

- Any member of staff employed by the School who comes across an e-safety issue does not investigate any further but immediately reports it to the Senior Leadership Team and impounds the equipment. This is part of the School safeguarding protocol (If the concern involves the E-safety Co-ordinator then the member of staff should report the issue to the Headteacher).

Incident Reporting

Any e-safety incidents must immediately be reported to the Deputy Headteacher, Pastoral (if a member of staff) or the Senior Leadership Team or PDM (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

ICT Acceptable Use Policy for School Staff

I confirm that I have read and understood this ICT Acceptable Use Policy for School Staff and that I will use all means of electronic communication equipment provided to me by the School and any personal devices which I use in accordance with this document. In particular

1. Any content I post online (including outside School time) or send in an email will be professional, responsible and maintain the reputation of the School. I will not make or post indecent remarks, proposals or material on the internet including racist or sexist jokes and defamatory comments. I will not send inappropriate messages.

2. I will reject requests / invitations from students to partake in social forums (such as Facebook, MySpace, and Blogging sites), instant messaging, and webcams. Equally, I will not make requests to students for them to join any of the above. Any communication with students on academic forums will be via the School's VLE or after discussion with senior staff.

3. I will not use social networking / purchasing sites (e.g. Facebook / Amazon/ E-bay) during contact time with students. I will not access or download inappropriate or illegal material. I will not try to bypass any filtering and security systems in place, or try to install private hardware / software (without gaining prior permission from the ICT Systems manager).

4. I will immediately report any accidental access to material which may be considered unacceptable to my line manager and ensure that it is recorded. Accessing or trying to access indecent images will be challenged and treated as a very serious breach of professional standards.

5. I will support the School approach to online safety and not deliberately upload or add any images, video, sound or text that could upset or offend any members of the School community.

6. I will take great care when deciding the appropriateness of photos/videos for the students I am teaching.

7. I will not give out personal details such as home / mobile number, personal email address; log in details to pupils, unless the need to do so is agreed with senior management in advance.

8. I will only use my School email address and School telephone numbers (including School mobiles) as contact details for pupils and their parents. I will not give out personal details (such as home phone number) unless this has been previously agreed with senior staff.

9. I will only use my personal mobile phone during non-contact time for incoming/outgoing calls. It will be kept on silent mode during assemblies / lessons except for staff that have specific responsibilities that need to be contactable.

10. I will not use personal mobile phones or other electronic equipment to photograph or video pupils unless parents have given their prior permission. I will not video or photograph staff without their individual permission.

11. I will ensure that I never use electronic communication as a means to bully or harass any members of the School community.

12. I will take all reasonable steps to ensure the safety and security of School ICT equipment which I take off site, and agree to the conditions as set out in the ICT loan agreement document that I will sign before

removing it from the School site. I will take all reasonable steps to ensure that memory sticks and personal ICT equipment brought into School are virus protected and that data within is secure.

13. I understand that personal ICT equipment used to access the School's BYOD (Bring Your Own Device) system will not be allowed to log into my personal account, and may only pass through the BYOD portal to access my files/emails.

14. I understand that I have a duty to protect my password and personal School log-ins. Any attempt to access, corrupt or destroy other users' data, or compromise their privacy in any way is unacceptable. I will aim to ensure that I log out of all computers when they are not in use.

15. I will ensure that confidential School information and pupil data will only be stored on a device that is encrypted or protected with a strong password. I will not leave a public machine logged on and unattended.

16. I understand that I have the same obligations to protect School data when working on a computer outside School. I will not give out staff / student's personal details, such as home phone number, unless this has been agreed with senior staff.

17. I will report immediately any accidental loss of confidential information so that appropriate action can be taken.

18. I understand that the School may monitor and check my use of ICT equipment and electronic communications. ICT use and access will be routinely logged.

19. I understand that I have a responsibility to report any misuses of technology by others.

20. I understand that by not following these rules I may be subject to the School's disciplinary procedures. This may range from informal warning through to dismissal.

Name (print)………………………………………………………………Date………………………..

Signed…….

STUDENTS' ACCEPTABLE USE OF ICT FOR THE KING'S SCHOOL NETWORK AND THE WORLD-WIDE WEB

When I use The King's School's ICT resources, I agree to the following Code of Conduct:

- I will use only my own username and password, when I log on.
- I will not tell any other person my password.
- I will not attempt to use someone else's username and password (even with their permission).
- I will only use the School ICT resources for School purposes.
- I will not download games or other programs from the web.
- I will not attempt to bypass security measures on the School network.
- I will not store music, games or videos in my user area.
- I will report any misuse, damage or vandalism of the School network to the ICT staff.
- I will only access websites that are appropriate for use in School.
- I will not take information from the web and pass it off as my own work.
- I will not use language in emails, text messages or other technology that could be seen as inappropriate, offensive or threatening.
- I will remember that everything that is sent out from The King's School carries The King's School email address and represents the School and its ethos, therefore I will be responsible in my use of email.
- I will not give out my or anyone else's personal details in an email, unless permission has been given.
- I understand that I may not use a mobile phone at School to take pictures or videos of staff or students, and then upload them onto Facebook, You-Tube or other similar social networking sites. If I do, I know that this may result in disciplinary action against me.
- I will always act responsibly with the School's Bring You Own Device (BYOD) network, and understand that this Code of Conduct also applies to the use of personal equipment on this network. I understand that any breaches of this Code will result in my removal from the BYOD network and possible disciplinary action.
- I understand that the School is not responsible for the care and security of BYOD devices and that these are brought to School solely at my own risk.
- I understand that if found using the School network or equipment in an inappropriate manner or damaging equipment, I will be banned from using the ICT facilities and disciplinary action will be taken against me, including requiring me to meet the cost of repair and/or replacement.

I am aware that ICT Monitoring software may be used on ALL computers at The King's School. The software runs in the background and may monitor keyboard inputs and internet use, identifying individual user, workstation and time.

Violations of this Acceptable Use of ICT Policy may be recorded and may be used in evidence, as part of any disciplinary or criminal proceedings.

This Acceptable Use of ICT Policy applies at all times, in and out of School hours, whilst using School equipment.

STUDENTS' ACCEPTABLE USE OF ICT FOR THE KING'S SCHOOL NETWORK AND THE WORLD-WIDE WEB

Pupil's name: ………………………………………………………………………………please print) Form………………….

I have read The King's School's Acceptable Use of ICT Policy, and agree to abide by the conditions of use.

Pupil's Signature: ……………………………………………………………………………………………………..

Parent/Carer's Signature: ………………………………………………………………………………………….

Date: ………

I have read The King's School's Acceptable Use of ICT Policy, and have discussed it with my son/daughter.

<u>Years 3-6</u>

Please return this slip to your son/daughter's Class Teacher.

<u>Years 7-11</u>

Please return this slip to your son/daughter's ICT Teacher.

<u>Sixth Form</u>

Please return this slip to the tray outside the UCAS Office.