



the *King's*
school

Safeguarding E-Communications Policy

Governor Committee Curriculum & Pupil Standards

E-COMMUNICATIONS POLICY

Policy Statement

The School's Safeguarding Policy ensures that The King's School is committed to protect the welfare of children and young people when they come into contact with the services that we provide. The E-Communications strand of the policy focuses on encouraging users to make effective and safe use of the School's computer network, multimedia materials, electronic communications and the Internet. Such use should always be safe, lawful and appropriate. It should not compromise users' sensitivities, The King's School's information and computer systems nor have the potential to damage The King's School reputation.

Purpose

This policy seeks to:

- Ensure that the Internet and electronic communications are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk;
- Clarify The King's School framework for using multimedia materials and electronic communications within the curriculum;
- Provide The King's School's employees with clear guidance on the rules of acceptable use of electronic communications and multimedia materials;
- Uphold copyright laws with regard to using multimedia materials within the curriculum;
- Inform students and parent(s)/carer(s) about The King's School rules for acceptable use of multimedia materials and electronic communications within the curriculum.

Scope

This policy applies to all users, students, staff, and administrators of The King's School computer network. It will also cover use of multimedia materials by other people with the students, either within or outside of the campus.

On evidence provided by The King's School, a user as defined above, may be disciplined by the Governing Body of the school. At the same time, if a user's conduct and/or action(s) are illegal, the user may become personally liable in some circumstances. (See Appendices)

Disclaimer

The Internet is a worldwide network of computers that contains millions of pages of information and provides users with a wealth of research materials. Users are cautioned that many of these pages include offensive, sexually explicit and inappropriate material. In general it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address may lead to the receipt of unsolicited e-mails containing offensive content. Users accessing the Internet do so at their own risk and The King's School is not responsible for material viewed or downloaded by users from the Internet and may apply suitable sanctions to any user who violates these protocols. To minimise these risks, use of the Internet at The King's School is monitored and filtered by the ICT Support Team.

Responsibility

Staff - All staff are expected to:-

- Read and abide by the terms of the policy;
- Explain the policy terms to students and visitors;
- Ensure that staff and students comply with the terms of the policy;
- Engage with policy evaluation.

Students - All students are expected to:-

- Comply with the terms of the policy;
- Engage in school surveys related to monitoring and evaluation of the implementation of the E-Communications Policy.
- Report any violation of the policy terms to a member of the Senior Leadership Team.

Visitors - All visitors of The King's School are expected to:-

- Read the King's School E-Communications Policy when the need arises;
- Abide by the terms of the policy.

Leadership and Management - Members of the Senior Leadership Team are expected to:-

- Ensure that all staff are adhering to the policy;
- Monitor the use of the E-Communications Policy;
- Review and evaluate the terms of the policy in consultation with stakeholders.

Publicity

A statement regarding the E-Communications Policy will be made on all publicity materials. All new staff and students recruited to the School will be made aware of the Policy. The Policy will be posted on the Shared (G) drive of the School's IT Network and the School's website.

POLICY GUIDANCE (Internet acceptable use, E-mail, Online social communication, Real time online communication and Misuse of electronic equipment)

Use of Internet facilities

For the purposes of this document, Internet usage means any connection to the Internet via Web browsing, external email or news groups. The King's School expects all users to use the Internet responsibly and strictly according to the following conditions:

Users shall not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Pornography (including child pornography);
- Promoting discrimination of any kind;
- Promoting racial or religious hatred;
- Promoting illegal acts;
- Any other information which may be offensive to colleagues or other students.

The King's School acknowledges that in certain planned curricular activities, access to sites otherwise deemed inappropriate may be beneficial for educational use (for example investigating racial issues).

Any such access should be preplanned and recorded so that it can be justified if required.

Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative;
- Adult material that potentially breaches the Obscene Publications Act in the UK;
- Criminally racist material in the UK.

If inappropriate material is accessed accidentally, users should immediately report this to The ICT Support Team so that this can be taken into account for monitoring purposes.

Also, users should not:

- Use The King's School facilities for running a private business;
- Enter into any personal transaction that involves The King's School in any way with the exception of personal items delivered to the school address;
- Visit sites that might be defamatory or incur liability on the part of The King's School or adversely impact on the image of the school;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside The King's School, or to The King's School itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic, sending or receiving of large files or sending and receiving a large number of small files or any other activity that causes network congestion, thereby substantially hindering other users of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.

Permitted Usage of Internet and E-mails

The computer network is the property of The King's School and may only be used for legitimate educational purposes. Users are provided access to the computer network to assist them in their educational, professional and personal development. All users have a responsibility to use The King's School's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet, may result in disciplinary action, including possible termination of user rights and civil and/or criminal liability.

Advice on E-mail Usage

WARNING: E-mail is neither private nor secret. Personal e-mails can easily be forwarded to other parties for whom they were not originally intended and the message manipulated or misconstrued. This can result in liability of the sender for issues arising such as sexual harassment, defamation or discrimination. ***E-mails are discoverable documents that may be required to be produced for legal proceedings should that be deemed necessary.***

All work-related emails should be written using a school e-mail address. School e-mail should be regarded as an official communication. E-mails should be written in the same professional tone and text as any other form of official school communication.

School e-mail accounts must not be used to send, store or circulate personal e-mail.

The sending of racially abusive or other offensive e-mail is forbidden and may be considered a criminal act. Bear in mind that emails may be submitted as evidence in legal proceedings and that e-mail discussions with third parties can constitute a legally binding contract.

A user should not access the e-mail of another user within the school without express permission and a clear understanding of the reason for the proxy access. However, users should be aware that school e-mail accounts may be accessed by other school staff for monitoring or management purposes as described in the monitoring section.

Users should not trust unsolicited external e-mails, especially any with file attachments. If in doubt, these should be deleted without opening the mail or saving any attachments.

Users should never reply to nor acknowledge receipt of external e-mail from unknown sources - this will only confirm to the sender that the user's e-mail address is valid, laying the user open to further unsolicited e-mail or the theft of their e-mail address for use in sending junk mail.

Users should also be aware that adding disclaimers to e-mail sent to external sources does not offer any legal protection to the sender.

Action you must take if in receipt of inappropriate emails

It is impossible to control what information is sent to a user by e-mail. However if offensive, obscene and/or discriminatory material is received it is then the responsibility of the receiver to report immediately, and in writing, to the designated person in school (or the Headteacher). Never send a reply.

Keep a printed copy of the e-mail as evidence and pass a copy of the e-mail to the appropriate person for the record. Ensure that the sender's information is also recorded as their email service provider may take action.

Monitoring

The King's School ICT Support Team will monitor and audit the use of the Internet to see whether users are complying with the policy. Any potential misuse identified by The ICT Support Team will be reported to the Headteacher and/or relevant organisation.

Online social communication such as social networks, blogs

Many staff and students use the computer for social communication outside school. (e.g. Facebook, Instagram and WhatsApp) Staff **SHOULD NOT** use school facilities to access or update personal social networks. Staff should be aware of the potential risk to their professional reputation of adding students, parents or friends of students as 'friends' on their social network site and are strongly recommended not to do so.

Care should be taken that comments made on a social network site or blog do not relate to or identify the school, staff or students as this could result in disciplinary action. It is also important that photographs and descriptions of activities in the personal life of staff do not adversely affect the professional reputation of staff or the school. Staff should be aware that even if they have used the privacy settings, they may not be able to prevent material becoming public from 'friends' sites.

It is recognised that online social communications tools, such as blogs and Wikis, have a potentially useful role in schools - such as on school websites, learning journals, celebrating good work, sharing information and facilitating collaboration. Where students and their families are sharing these tools with staff in school it is important that this should always be through a school based provision, such as the school Learning Platform, using a school log-in where all communication is open and transparent.

If staff keep a personal blog the content must maintain acceptable professional standards. Any inappropriate use may lead to disciplinary action in accordance with school policy. All blogs should contain a disclaimer that the views expressed are personal and not necessarily those of the school.

Any School is vulnerable to material being posted about them online and all users should be aware of the need to report this should they become aware of anything bringing the school into disrepute.

Action you must take if you discover inappropriate, threatening or malicious material online concerning yourself or your school

Secure and preserve any evidence. For example note the web address (URL) or take a screen shot or copy and print the screen.

Report immediately to relevant staff or the Headteacher.

Contact the uploader of the material or the Internet Service Provider/ site administrator and ask for the material to be removed. *All social network sites have the means to report unacceptable material or activity on their site - some more readily available than others. If the material has been created by a school user then the school has a responsibility to deal with it.*

Real time online communication e.g. Twitter, texting, using web cameras, chat, mobile phone

The ability to communicate in real time using the computer and other electronic devices (such as mobile phones) makes these an excellent tool for a range of educational purposes. However staff and students should take the same level of care with these tools as they would if working in a face to face situation. Access should always be through a school created account, never a personal account and it should be focused on a clearly specified educational objective.

There are likely to be times when this kind of activity will happen outside normal school hours and off the school premises. In this situation it should always be carried out with the full knowledge and agreement of the relevant staff. Staff should be aware that they must remain focused on the educational purpose of the communication and never allow it to become a social exchange.

Staff should also agree to specific times for availability and only allow contact during these times, to protect their personal time. When a web camera is used it should have a clear purpose. Staff should be aware of the ability of meetings of this kind to be recorded without their knowledge. However they may wish to use this function for their own security, as long as all parties are informed that recording is taking place.

Staff must protect their privacy by never allowing students or parents to obtain their contact details such as a mobile phone number or login details. Cyberbullying of staff by students is very common by mobile phone or e-mail.

Action you must take if an incident occurs

- Report immediately and in writing to the relevant staff.
- Don't reply to abusive or worrying text or video messages.
- Don't delete messages. Keep them for evidence.
- Use 1471 to try and obtain the number if you can. Most calls can be traced.
- Report it to your phone provider and/or request a change of number.
Technical staff may also be able to help you to find or preserve evidence e.g. logs of the call.

Misuse of electronic equipment

Misuse can be a serious disciplinary offence. The following examples of misuse apply to all users in The King's School.

Users **MUST NOT** use school equipment (including a school provided laptop) to:

- Store, view, download or distribute material that is obscene, offensive or pornographic, contains violent images, or incites criminal behaviour or racial hatred;
- Gamble;
- Undertake political lobbying ;
- Promote or run a commercial business ;

- Download or distribute games, music or pictures from the internet for personal use. They can bring viruses with them, use up capacity on the servers and potentially breach copyright;
- Spend school time on personal matters (for example, arranging a holiday, shopping, looking at personal interest websites). This may be treated as fraud;
- Store personal information on the school network that uses up capacity and slows down the system (for example, personal photos, screensavers or wallpaper);
- Send e-mails, texts or messages or publish anything on a website, social networking site or blog, which:
 - Is critical about members of the school community;
 - Contains specific or implied comments you would not say in person;
 - Contains inappropriate comments which could cause offence or harassment on the grounds of gender, race, disability, age, religion or sexual orientation.
- Conduct private and intimate relationships via school systems;
- Download or copy software (excluding software updates) or use the e-mail system to transmit any documents or software without checking copyright or licence agreement;
- Install software licensed to the school on a personal computer unless permission to do so is explicitly covered by the school licence agreement;
- Take, transmit or publish pictures of a member of staff or student on a mobile phone, camcorder or camera without the person's permission;
- Give away e-mail lists for non-school business. If in doubt, ask your Headteacher or other relevant staff;
- Use internet chat rooms (other than the secure, moderated facilities which are provided within the school's Learning Platform).

A **personal laptop** brought onto the school premises **MUST NOT** be used to undertake any of the above activities during the school day, nor should it have information stored within it which would be deemed to be unacceptable on a school machine. It is recommended that a personal laptop used at school should have a separate secure account for school use. Additionally a personal laptop used for any school activity must be fully protected against virus infection.

POLICY GUIDANCE (Multimedia materials)

- Certification of some multimedia materials is divided, generally, into six categories: U (universal) - suitable for all: PG (Parental Guidance) - some scenes may be more disturbing for younger viewers and parents should exercise caution and judgement in showing the material to younger viewers: 12 - children of 12 or over only: 12A - children under the age of 12 can watch the multimedia materials only with parents or carers: 15 - children under 15 may not watch the multimedia materials - only adults 18 or over can watch the multimedia materials. These certifications are awarded by the British Board of Film Certification (BBFC) and are legally binding for cinemas and retail outlets. However, for domestic use the certification is a guideline that parents can exercise judicious care with.
- Departments should ensure that the use of any multimedia materials generally falls in line with the chronological age of the students in the class. The multimedia materials should form part of the curriculum and must be relevant to the unit of study. However, there are occasions on which multimedia materials shown will be beyond the age of the students involved.

On these occasions teachers must exercise the same judicious care that parents at home would exercise in deciding if multimedia materials are appropriate to support study.

- Any multimedia materials from sources beyond chronological age of students should be especially used with care in the curriculum, and teachers should consider carefully the reasons for using these materials. The extracts which attract the certification (which are usually stated on the box) should be avoided. If it is not possible to avoid these extracts then a letter should be sent home to the carers of students in the class concerned, seeking permission to allow their children to view the relevant material. This letter should outline the teacher's reasons for using these extracts and offer parents who do not agree the chance to withdraw their students from the classes in which they will be shown, without prejudice. This procedure should also be followed for all students where the chronological age of the students is below the age of the certification awarded.
- Where multimedia materials beyond the chronological age are used they must be studied in context. The teacher has a duty to bear in mind the issues which arise (violence, drug taking, foul and abusive language, etc) and contextualise them for the class. This is part of the wider understanding of the world around them which pupils should gain from the use of such material, as well the technical and curricular specific areas of study. Teachers should highlight this capacity for a wider discussion of issues of citizenship within the planning for the lesson.
- Should a teacher plan to use any multimedia materials in its entirety or as the basis for an entire lesson, then this should be of an appropriate certification for the age of the students in the class, other than where exceptional circumstances apply. Again, if the certification exceeds the chronological age of the students in the class then a letter of parental consent must be issued prior to the use of the materials.



Staff Acceptable Use Agreement

To ensure that staff are fully aware of their responsibilities with respect to ICT use, they are asked to sign this acceptable use agreement.

- I understand that the network is the property of the School and agree that my use must be compatible with my professional role.
- I understand that the School ICT systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that use for personal financial gain, gambling, political purposes or advertising is not permitted.
- I understand and agree that the School may monitor my network and Internet use to ensure policy compliance.
- I will not install any software or hardware without permission.
- I will not disclose any password or login name to anyone, other than, where appropriate, the ICT Support Team.
- I will take all reasonable precautions to secure data or equipment taken off the School premises. Any student data in a member of staff’s possession outside of the network domain must be kept secure eg. Copied to a memory stick that uses encryption to save data.
- I will report any incidents of concern to the School’s Designated Child Protection Co-ordinator or E-Safety Co-ordinator as appropriate.
- I will ensure that my electronic communications with students are compatible with my professional role and cannot be misinterpreted. When using social networking sites (Facebook, MySpace etc.) staff should **NOT** have current King’s School students as “Friends”.
- I will promote e-safety with the students that I teach and will help them to develop a responsible attitude to ICT use.
- I will respect copyright and intellectual property rights.

The School may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the School's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed:

Capitals:

Date:



Dear Parent(s)/Carer(s)

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, The King's School is providing supervised access to the Internet. We believe that the use of The World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Although there have been national concerns about students having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home, in which case we can provide information on safe access to the Internet, including an article on the School website.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the accessibility of inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please telephone me to arrange an appointment.

Yours sincerely

Barbara Tibbetts
Headteacher

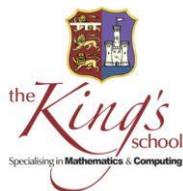


RESPONSIBLE INTERNET USE

We use the school computers and Internet for learning. These rules help us to be fair to others and keep everyone safe.

- I will ask permission before entering any website, unless my teacher has already approved that site.
- On a network, I will use only my own login and password, which I will keep secret.
- I will not look at or delete other people's files.
- I will not bring memory sticks or portable hard disks into school without permission.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or e-mail attachments sent by someone I do not know.
- I will not use Internet chat sites or social networking sites such as Facebook, MSN etc.. without any teacher supervision.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.
- I know the school will check my computer files and monitor the Internet sites I visit.
- I know that if I deliberately break these rules I could be stopped from using the Internet and computers.

The School may exercise its right by electronic means to monitor the use of the School's computer systems, including the monitoring of websites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the School's computer systems is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery text or imagery which is unauthorised or unlawful.



The King's School Responsible Internet Use

Please complete, sign and return to the Form Tutor

Student Name:

Tutor Group:

Student's Agreement:

I have read and understood the School Rules for Responsible Internet Use. I will use the computer systems and Internet in a responsible way and obey these rules at all times.

Signed: Date:

Parent(s)/Carer(s) Consent for Internet Access:

I have read and understood the School Rules for Responsible Internet Use and give my permission for my son/daughter to access the Internet within the School. I understand that the School will take all reasonable precautions to ensure that students cannot access inappropriate materials. I understand that the School cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the School is not liable for any damages arising from use of the Internet facilities.

Signed: Date:

Please print name:

Parent(s)/Carer(s) Consent to Web Publication of Work and Photographs:

I agree that, if selected, my son's/daughter's work may be published on the School Website.

I agree that photographs that include my son/daughter may be published subject to the School Rules that names will not be used with photographs to identify individuals.

I do **NOT** agree to my son's/daughter's work or photographs including my son/daughter being published on the website.

Please indicate by ticking the relevant box (es)

Signed: Date: