THE KING'S SCHOOL

GRANTHAM

E-Safety Policy

Aims

To ensure that students and staff are able to use the internet and related communication technologies appropriately and safely.

To build students' and staff resilience to risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

To provide the necessary safeguards to manage and reduce risks.

Help students and staff to be responsible users and stay safe using the internet and other communication technologies for educational, personal and recreational use.

To safeguard students and staff.

Scope Of The Policy

This policy applies to all members of the school community who have access to and are users of school IT systems – staff, students, volunteers, parents, visitors.

Context

The internet and other digital and information technologies are powerful tools. Young people should have an entitlement to safe internet access. Though the use of these innovative technologies can help to raise educational standards, nevertheless they can also put young people at risk. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images.
- Unauthorised access to personal information.
- The risk of being groomed by those with whom they make contact on the internet.
- Sharing or distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication or contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video or internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of students.

It is impossible to eliminate risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the skills and confidence to deal with these risks.

Policy adopted: January 2018
Reviewed: February 2018
Next Review: January 2023

Roles and Responsibilities

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy.

Head Master

Ensuring the safety of members of the school community, though the day to day responsibility will be delegated to the IT technician.

Make sure there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.

Receive regular monitoring reports from the IT technician.

Implement the policy in the event of a serious e-safety allegation being made against a member of staff.

IT Technician

Takes day to day responsibility for e-safety issues.

Liaises with school staff.

Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety event taking place.

Ensure that staff are advised on e-safety issues.

Maintains a log of incidents.

Reports to the Head Master on e-safety issues.

Network Manager

Make sure the IT infrastructure is secure and not open to misuse or malicious attack.

Make sure users can only access the school's networks through a properly enforced password protection system.

Keeps up to date with e-safety technical information.

Regularly monitors the network in order that any misuse or attempted misuse is reported to Deputy Head Master or Head of Sixth Form.

Teaching and Support Staff

Read and understand the e-safety policy.

Read and understand the Staff Acceptable Use Policy (AUP).

Report any suspected misuse or problem to the IT technician or Head Master.

Digital communication with students should always be on a professional level and only carried out using school systems.

Ensure students understand and follow the school e-safety and Acceptable Use Policy.

Ensure students understand research skills and the need to avoid plagiarism and uphold copyright regulations.

Monitor IT activity in lessons.

Be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices.

In lessons, guide students 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.

The school may monitor use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes inappropriate use of the school's system is or may be taking place, or the system is or may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Designated Safeguarding Lead (DSL)

Be aware of the potential for serious child protection issues to arise from:

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

Parents/Carers

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

The school will help parents to understand e-safety issues through newsletters, the school website and involvement in local e-safety campaigns.

Parents should be aware of the school policy on e-Safety and the School Acceptable Use Agreements which are available on the school website.

Students

Are responsible for using the school IT systems in accordance with the Student Acceptable Use Policy.

Have a good understanding of personal research skills and the need to avoid plagiarism and uphold copyright regulations.

Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Expected to know and understand school policies on the use of Mobile Phones, Smart Watches, Personal Portable Electronic Devices and Other Electronic Devices Policy. They should know and understand school policies on the taking and use of images and on cyber-bullying.

A planned e-safety programme will be provided as part of the IT programme.

Assemblies will re-visit the issue of e-safety.

Students, where appropriate, should be taught to be critically aware of the materials they access and be guided to validate the accuracy of information.

Students should be encouraged to adopt safe and responsible use of IT and to respect copyright when using materials accessed on the internet.

The school may monitor use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes inappropriate use of the school's system is or may be taking place, or the system is or may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Technical Infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

There will be regular reviews and audits of the safety and security of school IT systems.

Servers, wireless systems and cabling must be securely located and physical access restricted.

All users will have clearly defined access rights. Details of the access rights will be recorded by the Network Manager.

All users will be issued with a username and password by the Network Manager. Users are responsible for the security of their username and password.

The school maintains and supports a managed filtering service.

School IT technical staff regularly monitor and record the activity of users on the school IT systems.

Appropriate security measures are in place to protect servers, firewalls, routers, wireless systems, work stations and hand held devices from accidental or malicious attempts which might threaten the security of the school systems and data.

Temporary access for guests is available. This has very limited access.

The school infrastructure and individual workstations are protected by up to date virus software.

Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

The school uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming and chat rooms.

Use of digital and video images

Staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet.

The school will inform and educate students and staff about the risks associated with the taking, use, sharing, publication and distribution of digital images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

The school recognises that staff may use personal portable electronic devices to record legitimate images provided these are then uploaded to the appropriate location within the school's network or website and then deleted form the member of staff's device at the earliest convenient opportunity.

Care should be taken whilst taking digital/video images that students are appropriately dressed.

Students and staff must not take, use, share, publish or distribute images of others without their permission, or in the case of a student under the age of 13 without parental permission.

Students' full names will not be used anywhere on the website, particularly in association with photographs without first having the permission of parents and the Head Master.

Written permission from parents will be obtained before photographs of students are published on the school website.

The school blocks access to social networking sites.

We have CCTV in school as part of our site surveillance for student and staff safety. The use of this is covered in the specific policy.

E-mail

The school email service is regarded as safe and secure and is monitored.

Users must immediately report to their teacher, Head of Year, Designated Safeguarding Lead or Head Master if they receive any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to such material.

Any digital communication between staff and students, pupils or parents, must be professional in tone and content.

Personal email addresses, text messaging or public chat or social networking programmes must not be used for these communications.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Email must not be used by staff to transfer information to a third party about students - unless it is within an encrypted, secured email system.

Protecting Personal Data

Personal Data will be recorded, processed, transferred and made available according to the GDPR.

Responding to incidents of misuse

In most cases, the IT Technician should be the first point of contact for any incident of misuse.

Any complaint about staff should be reported to the Head Master.

Complaints about cyber-bullying are dealt with in accordance with the school Anti-Bullying Policy.

Complaints related to Child Protection are dealt with in accordance with the school Safeguarding Policy and should be referred to the Designated Safeguarding Lead.

Incidents of mobile phone misuse will be dealt with in accordance with the school Mobile Phone, Smart Watches, Personal Portable Electronic Devices & Other Electronic Devices Policy.

Monitoring and review process

The Head Master will monitor the implementation of the policy and report to governors about e-safety incidents and any significant new developments in his report to the full Governing Body.

APPENDIX 1

Student Acceptable Use Policy (SAUP)

All students are expected to abide by the rules designed to keep everyone safe. All students should:

- Never share their password with anyone, or use anyone else's password. If they become aware of another individual's password, they should inform the person and a member of staff.
- Use a 'strong' password – one that contains letters (upper and lower case), numbers and possibly symbols which will be changed on a regular basis.
- Use school equipment properly and not interfere with the work or data of another student.
- Understand that the school may check computer files and will monitor internet sites visited.
- Before connecting their own equipment to the school network; check with a member of staff to see if it is allowed.
- Use storage devices appropriately.
- Understand that they are responsible for all email, chat, SMS (Short Message Service) blogs etc. that they post or send and use language appropriate to the audience who may read them. They should be respectful in how they talk to and work with others online and never write or participate in online bullying. Report any unpleasant material or messages sent to them. Understand their report will be confidential and may help protect other students and themselves.
- Know that posting anonymous messages and forwarding chain letters is forbidden.
- Understand that files attached to an email will be appropriate to the body of the email and not include any inappropriate materials or anything that threatens the integrity of the school IT system.
- Never download or bring into school unauthorised programs, including games and music and run them on school computers.
- Never access inappropriate materials such as pornographic, racist or offensive material or use the school system for personal financial gain, gambling, political purposes or advertising.
- Never give their home address, mobile phone or telephone number, or arrange to meet someone, unless their parent or carer has given permission when using social media.
- Always use the terms and conditions when using a site. Know that content on the web is someone's property and ask a responsible adult if they want to use information, pictures, video or music or sound to ensure they do not break copyright law.
- Think carefully about what they read on the internet to question if it is from a reliable source before they use the information.
- Always credit sources so that they avoid plagiarism.
- Never make audio or video recordings of another student or teacher without his/her permission.

APPENDIX 2

Staff (And Volunteer) Acceptable Use Policy (AUP).

In order to safeguard students and colleagues it is important that staff take all possible measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All colleagues have a responsibility to use the school's computer system in a professional, lawful and ethical manner. All staff and volunteers should:

- Use school-owned information systems appropriately. Understand that the Computer Misuse Act makes the following criminal offences:
    - to gain unauthorised access to computer material;
    - to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- Understand that any hardware and software provided by the school for staff use can only be used by members of staff and only for educational use.
- Prevent unauthorised access to systems or personal data, not leave any information system unattended without first logging out or locking their login as appropriate.
- Respect system security and not disclose any password or security information. Use a 'strong' password (including letters and numbers).
- Never attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- Ensure that any personal data of students, staff or parents is kept in accordance with the GDPR and school Data Protection Policy.
- Never keep professional documents which contain school-related sensitive or personal information (including images, files or videos) on any personal devices unless they are secured and encrypted.
- Never store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- Never attempt to bypass any filtering or security systems put in place by the school. Report all suspected computer system damage, virus or other malware to the IT Network Manager.
- Understand that use of the school information systems, internet and email may be monitored.
- Electronic communications with students, parents and other professionals will only take place via work approved communication channels. Any pre-existing relationships which may compromise this should be discussed with the Head Master.
- Email should be treated in the same way as any other form of written communication. Anything put in an email is potentially disclosable. You should not include anything in an email which is not appropriate to be published generally.
- Where possible, avoid blanket emails. You should be aware that emails are disclosable as evidence in court proceedings and, even if they are deleted, a copy may exist on a backup system.
- Encrypt electronic records where possible.
- Promote e-safety with students and help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- Unsuitable material: viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material the school believes is unsuitable is strictly prohibited and constitutes gross misconduct. This includes such at any time on the school's networks or via 3G or 4G when on school premises. Internet access may be withdrawn

without notice at the discretion of the Head Master whilst allegations of unsuitable use are investigated.

- Do not show SIMs registration data to the whole class. If your projector is on then use the freeze function on the remote to ensure privacy.
- Do not show whole class assessment data to the rest of the class.
- USB sticks - encrypt where possible. Use for planning and teaching resources only. Do not store identifiable student or staff data on USB sticks. You need to think about how you keep your USB stick safe.
- The school must keep its systems secure to avoid personal data being hacked.
- Photographs – make sure students and parents have given their permission for the photographs to be used.
- Home Computer – if you use it for school work, please ensure that it is up to date with anti-virus software. Do not save personal data or sensitive data at home.
- Respect copyright and intellectual property rights.
- Read and understand the school e-Safety Policy.
- Report all incidents of concern to the Designated Safeguarding Lead (DSL) and/or the Head Master.

Sign: .....

Print: .....

Date: .....

APPENDIX 3

Safeguarding of School Staff -Electronic Communications with Students Including the Use of Email and Social Networking Sites

All adults employed in the school should:

- Ensure that personal social networking sites are set as private and students should never be listed as approved contacts.
- Never use or access the social networking site of any student unless for investigative purposes (only Heads of Year, Designated Safeguarding Lead or SLT).
- Personal contact details should not be given to students, including mobile telephone numbers.
- Only make contact with students for school-related business, eg extra-curricular activities.
- Recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible.
- Never use Social Media to send personal messages to a student.