King's Norton Boys' School

E-safety Policy

Adopted by the Governing Board: July 2017
To be reviewed by: July 2018

This Policy has been adopted by the Governing Board of King’s Norton Boys’ School:

Signed by:

_________________________ Headteacher Date: _____________________________

_________________________ Chair of governors Date: _____________________________

King's Norton Boys' School recognises the need to maintain a strategy for effective use of the Internet as a valuable tool for learning, to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. It also recognises the need to protect users, in particular young people, from offensive and dangerous material and acknowledges the need to ensure that all users make responsible use of the Internet.

Rationale

Significant educational benefits should result from curriculum Internet use, including access to information from around the world and the ability to communicate widely. Internet safety depends on staff, governors, advisers and parents to take responsibility for the use of the Internet.

The Internet is an essential element in 21st Century life for education, business and social interaction. KNBS has a duty to provide students with quality Internet access as part of their learning experience. The purpose of Internet use in school is to raise educational standards, to promote student achievement and to support the professional work of staff.

E-safety covers the Internet as well as mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any person working with children and educating all members of the school community on the risks and responsibilities of E-safety falls under this duty. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Governors

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy by reviewing E-safety incidents and monitoring reports. Governors should:

- Ensure an E-safety Policy is in place, reviewed every 3 years and is available to all stakeholders.
- Ensure that there is an E-safety Co-ordinator who has received appropriate CEOP training.
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to.
- Hold the Head teacher and staff accountable for E-safety.

Head teacher and SLT

The Head teacher has a duty of care for ensuring the safety (including E-safety) of members of the school community, though the day-to-day responsibility for E-safety will be delegated to the ICT Network Manager. Any complaint about staff misuse must be referred to the ICT Network Manager at the school or, in the case of a serious complaint, to the Head teacher. The Head teacher should:

- Ensure access to induction and training in E-safety practices for all users.

- Ensure appropriate action is taken in all cases of misuse.
- Receive monitoring reports from the E-safety Co-ordinator.

E-safety Lead / ICT Network Manager

The E-safety Lead should:

- Lead on E-safety.
- Report to the Senior Leadership Team to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- liaise with the nominated member of the Governing Board & Head teacher to provide an annual report on e safety
- Ensure that the schools technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensure that the school meets required E-safety technical requirements eg. data protection, information security etc
- Check that users may only access the networks and devices through a properly enforced password protection policy.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person. (Smoothwall)
- Keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant.
- Monitor the use of the all school systems in order that any misuse can be reported to the Head teacher; E-safety Co-ordinator for investigation.
- Monitor software systems as agreed in school policies.
- Ensure that student or staff personal data as recorded within the school management system sent over the Internet is secured.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.

Guidance for All Users

Staff are encouraged to use ICT resources in their teaching and learning activities, to conduct research, and for contact with others in the education world. Electronic information-handling skills are now fundamental to the preparation of citizens and future employees in the Information Age. Staff are encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend its use, as appropriate, within the curriculum. They should model appropriate and effective use, and provide guidance and instruction to students in the acceptable use of the Intranet/Internet.

When using the Internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity and all school staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector.

Students are responsible for their good behaviour on the KNBS network, just as they are on and off school premises. While the use of information and communication technologies is a required aspect of the National Curriculum, access to the Intranet/Internet is a privilege – not a right. It will be given to students who act in a considerate and responsible manner, and may be withdrawn if they fail to maintain acceptable standards of use.

The school must ensure that both staff and students have read, understood and signed the ICT Acceptable Use Policy and that all users adhere to the terms. Users must not:

- Retrieve, send, copy or display any inappropriate material.
- Use obscene or racist language.
- Harass, insult or attack others.
- Damage computers, computer systems or computer networks.
- Violate copyright laws.
- Use another user's password.
- Trespass in another user's folders, work or files.
- Use the network for commercial purposes.

The benefits of using ICT and the Internet in schools

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between students all over the world.
- Access to subject experts, role models, inspirational people and organisations.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

Online activities which are encouraged include:

- The use of email and computer conferencing:
- Use of the Internet to investigate and research school work.
- Use of the Internet to investigate careers and Further and Higher education.
- The development of students' competence in ICT and research skills.
- Staff professional development through various on-line resources.
- Communication with support services, professional associations and colleagues.

- Exchange of curriculum and administration data with the LA and DfE.

Online activities which are not permitted include:

- Searching, viewing or retrieving materials that are not related to the aims of the curriculum or future careers.
- Copying, saving or redistributing copyright-protected material, without approval.
- Subscribing to any services or ordering any goods or services, unless specifically approved by KNBS.
- Playing computer games or using interactive ‘chat’ sites unless specifically approved by KNBS.
- Publishing, sharing or distributing any personal information such as home address, email address, phone number etc.
- Accessing public or unregulated chat rooms or arranging to meet with others via such means.
- Any activity that could potentially bring the school’s reputation into disrepute.

Supervising and Monitoring Usage

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The ICT Manager and IT Technicians will review the security of the school information systems and users regularly and virus protection software will be updated regularly. The ICT Network Manager should:

- Ensure that all personal data sent over the Internet or taken off site is encrypted eg laptops.
- Make sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this.
- Regularly check files held on the school network for viruses.
- Enforce the use of user logins and passwords to access the school network.

It is an absolute requirement that access to the Internet provided to staff and students through any Internet Service Provider (ISP) is a filtered service.

All users should be aware that the ISP and the school’s internal infra-structure can and does track and record the sites visited and the searches made on the Internet by individual users. The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of students. If users discover unsuitable sites then the URL will be reported to the ICT Manager. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

KNBS advises parents that they provide filtered and monitored access to the Internet for students. However, parents should also be aware that with emerging and constantly changing technologies there is no absolute guarantee that a student cannot access materials that would be considered unsuitable. The chance of just coming across such materials is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort an individual puts into their search. If a student is unfortunate enough to come across any offensive web pages, whilst using school equipment, they are obliged to make a note of the address and report it to the classroom teacher.

Teachers should guide students toward appropriate materials on the Internet. This will avoid a great deal of time wasting as well as going some way towards monitoring the sites accessed by students.

Internet access for students at KNBS is available on computers in all areas such as classrooms, libraries and study rooms. Machines, which are connected to the internet, should be in full view of people circulating in the area.

While using the Internet at KNBS, students should be supervised. However, when appropriate to their age and their focus of study, students may pursue electronic research independent of staff supervision. This should be at the discretion of the teacher in charge. No student should use school access to the internet unsupervised. In all cases students should be reminded of their responsibility to use these resources in line with the school policy on ICT / Acceptable Use.

Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls users must not expect files stored on KNBS school servers or within the Office365 system to be absolutely private. An email is as private as a postcard, it is quite likely that no one other than the sender and receiver will ever read it, but others could if they were inclined.

Emails

The school uses email internally for staff and students, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- Initiating contact and projects with other schools nationally and internationally.
- Providing immediate feedback on work, and requests for support where it is needed.

Staff and students should be aware that school email accounts should only be used for school-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents.

School Email Accounts and Appropriate Use

Students are assigned school email addresses that do not state their full name as this makes them more vulnerable to being identified by unsuitable people.

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.

- Staff must tell their line manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

Students should be aware of the following when using email in school: and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- In school, students should only use school-approved email accounts
- Social emailing will be restricted
- Students should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with these themselves.
- Students must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Students will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published.

Management of Web site content

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or students' home information will not be published.
- Web site photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' names will not be used on the Web site in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- The Head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Policy and Guidance of Safe Use of Children’s Photographs and Work

The use of colour photographs and students work is an important aspect of the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material. Under the Data Protection Act 1998 images of students and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school’s policy on the use of photographs of children, including:

- How and when the photographs will be used
- How long parents are consenting the use of the images for

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school’s permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all school publications
  - on the school website
  - in newspapers as allowed by the school
  - videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (ie a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of a child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students. For more information on safeguarding in school please refer to KNBS child protection and safeguarding policy**.**

Complaints procedures regarding Internet use or Misuse of Photographs or Video

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Students and parents will be informed of the complaints procedure.
- Parents and students will need to work in partnership with staff to resolve issues
- Parents / Carers should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs.

Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

Mobile Phones and Personal Device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make students and staff more vulnerable to cyberbullying
- Can be used to access inappropriate internet material
- Can be a distraction in the classroom
- Are valuable items that could be stolen, damaged, or lost

- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

Students may bring mobile phones to school, however, they should be turned off and out of sight during all lessons and formal time. Students may use their mobile phones sensibly in school, during break and lunch times only. Occasionally, and only with the absolute permission of a teacher, students may use their mobile phones during lessons as a learning resource.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined below.

- The school will not tolerate cyber bullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined.
- A member of staff can confiscate a mobile phone, and a member of the senior leadership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Mobile phones must be switched off during school lessons or any other formal school activities.
- Any student who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged. Images or files should not be sent between mobile phones in school.
- If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

Mobile Phone or Personal Device Misuse

Students

- Students who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.
- Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the student being prohibited from taking that exam.

Staff

- Under no circumstances should staff use their own personal devices to contact students or parents either in or out of school time.
- Staff are not permitted to take photos or videos of students on their personal devices. If photos or videos are to be taken as part of the school curriculum or for a professional capacity, then school devices must be used for this.
- Once photos or videos have been taken on a school device, they must be transferred into the school's central storage system and then deleted from the portable device at the very earliest opportunity.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.

- Any breach of school policy may result in disciplinary action against that member of staff.

<u>Cyberbullying</u>

The school, as with any other form of bullying, takes Cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the KNBS Behaviour Policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff.

If an allegation of cyber bullying does come up, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our **anti-bullying policy.**

Repeated bullying may result in fixed-term exclusion.

Management of Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- As stated earlier, mobile phones will not be used during lessons or formal school time unless permission is given by the classroom teacher for students to use them as an educational resource.

Protecting Personal Data

KNBS believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital. The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with GDPR, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate and up to date
- Not keep data longer than for the purpose it was originally collected
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.
- Ensure that data is destroyed securely

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Confidentiality

- Messages sent and received via the Internet are regarded by the Company's Act as having the same legal status as a corporate letter. Any material that is viewed as highly confidential or valuable to the School should not be e-mailed externally.
- A disclaimer document will be attached to all external e-mails with an individual signature for each user. In no instance should the disclaimer be tampered with, although if necessary the signature can be altered.
- It should be remembered that the Internet does not guarantee delivery or confidentiality.
- It should be noted that there are systems in place that can monitor, review and record all email usage, and these will be used. Analysis of this information may be issued to managers if thought appropriate. No user should have any expectation of privacy as to his or her email.