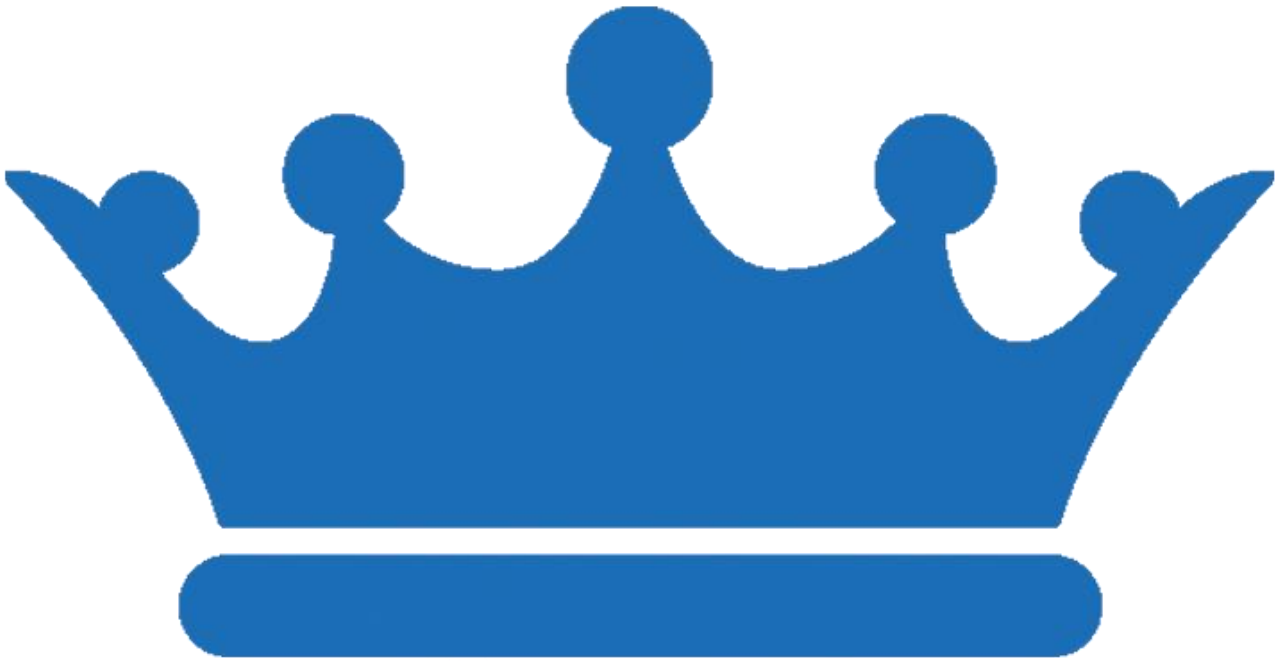
Kingsway Park
HIGH SCHOOL

E-Safety Policy

Reviewed Date: Feb 2020

Review Due: Feb 2021



Scope of this Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Kingsway Park High School.

This further extends to incidents of cyber bullying and other online safety incidents that may take place out of school but involve members of the school community.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where applicable, inform parents / carers / authorities of incidents of inappropriate online safety behaviour that take place through the school systems.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Network Manager / Technical Staff

The Network Manager and Technical Staff are responsible for ensuring the following:

- That the schools IT infrastructure is secure from misuse or attack.
- That the school meets all required online e-safety requirements.
- That they keep up to date with online safety technical information.
- That the use of the school IT systems including but not limited to Email, Internet, VLE and Remote Access are properly monitored for misuse or attempted misuse.

Teaching and Support Staff

Are responsible for ensuring that:

- They are aware of current online safety matters and of the schools current online / e-safety policies.
- They have read and understood all related Staff / School IT policies.
- They have reported any suspected misuse of IT or Computer systems.
- All digital communications with Students be on a professional level and only carried out using official school systems.
- All students follow the schools IT and other related polices.
- All students follow good practice for research, avoid plagiarism, and uphold copyright regulations.
- They monitor the use of digital technologies, mobiles, camera etc in lessons and other school activities and implement current policies with regard to these devices.
- They check all required digital resources for their suitability before allowing students to access them.

Students

All students are responsible for:

- Using the school IT system in accordance with prescribed IT / School policies and Acceptable Use Agreements.
- Not deliberately plagiarising work and for upholding copyright regulations.
- Reporting misuses or attempted misuses of the IT systems including the access of inappropriate materials.
- Knowing and understanding the policies on the use of mobile devices and other school equipment.
- Knowing and understanding the effects of cyber-bullying and for reporting any incidents they become aware of immediately whether they or another member of the school is the target.
- Understanding the importance of adopting good online safety practices when using all digital technologies in or out of school and to realise that the schools Online Safety Policy covers their actions out of school as well as inside the school.

Parents / Carers

Parents / Carers play a critical role in ensuring their children understand the need to use the internet and mobile devices in an appropriate way. As such, the school will take every opportunity to assist parents in understanding these issues. Parents / Carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital Photos and Videos
- Mobile Devices
- Social Media and the Internet

Policy Statements

Education - Students

Regulations and technical solutions are very important when it comes to online safety however, it is essential that these are used alongside the education of students in their online responsibilities and the correct use of IT and online systems. Therefore the education of students in online safety is an essential part of the schools online safety provision. With the support of the school, we hope that students will recognise and avoid online safety risks and build their resilience.

Since the internet is such an essential, part of modern life and education it is important that the message on online safety is covered cross-curricular and is reinforced by all staff as part of their curriculum.

Education - Staff

It is essential that all staff receive online safety guidance and understand their responsibilities as outlined in this policy. Guidance will be offered as follows:

- A planned programme of online safety drop-in sessions.
- All new staff should receive online safety guidance as part of their induction programme.

Technical

The school is responsible for ensuring that all IT infrastructure is as safe and secure as is reasonably possible and that policies and procedures are implemented to match legislation and school requirements. This includes:

- That the schools technical systems will be managed in ways that ensure that the school meets the recommended technical requirements.
- That regular reviews and audits on e-safety and security of technical infrastructure take place.
- That critical infrastructure is physically secure.
- That wireless systems are secured from unauthorised access.
- All users have clearly defined access rights on school systems and devices.
- That all users are provided with a username and password and they understand they are responsible their own account and security (i.e. not sharing usernames and passwords).
- That internet access is filtered for all users to prevent access to illegal or inappropriate content.
- That the internet filtering provides sufficient protection again terrorist and extremist material.
- That clear filtering levels / groups are maintained and that users only have access to material deemed acceptable / applicable to them.
- That school systems record and monitor the activity of users and those users are made aware of this fact.
- That appropriate systems are in place for the protection of key network infrastructure and that these are tested regularly to ensure there still effective.
- That an agreed policy is in place for temporary or guest access to the system.
- That a policy is in place regarding BYOD and /or personal devices.

Mobile Technologies (BYOD)

Mobile technologies are becoming more prevalent and present their own e-safety challenge certainly within the scope of BYOD. BYOD can include many digital devices including but not limited to:

- Smartphones
- Tablets
- Laptops
- Netbooks

Due to the nature of these technologies and the technical challenges they present Kingsway's current policy is for no student BYOD access.

BYOD access does exists in a limited manner for Staff in the forms wireless access for tablets and smartphones. This access exists to help facilitate access to key school systems such as email, VLE and remote applications.

Since these devices have access to the network staff need to be aware that all activity is monitored and filtered and that use / continued use of this network requires compliance with all IT and other school related polices.

Mobile Technologies (In house Devices)

The school operates a number of in-house mobile devices. These include but are not limited to:

- Laptops
- Netbooks
- IPads
- IPhones

Due to the nature of the setup of these devices and for the scope of this policy these are treated in the same way as any physical devices and all filtering and monitoring takes place in the same way.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In

particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images may only be taken on school equipment; the personal equipment of staff may not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Students' full names will not be used anywhere, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents / carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents

- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password-protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school, policy (below) once it has been transferred or its use is complete.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School Staff should ensure that:

- No reference should be made in social media to students, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Unsuitable / Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities, which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. These include but are not limited to the following:

- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour
- Promotion of extremism or terrorism
- Any other information, which may be offensive to colleagues, breaches the integrity of the ethos of the school, or brings the school into disrepute.
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Infringing copyright
- Revealing or publicising confidential or proprietary information
- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming (non-educational)
- On-line gambling
- File sharing
- Use of social media