King James's School

## POLICY STATEMENT

# E-Safety Policy

| | |
|---|---|
| Policy last reviewed (date) | June 2021 |
| Ratified by Governors (date) | June 2021 |
| Next policy review due (date) | June 2024 |
| Due for review by Governors (date) | June 2024 |
| Staff Lead | Senior Network Manager |

**MISSION STATEMENT:**

This policy will support the school by being reflective of the Governors' direction and School's development plan. It will be used in an efficient and effective manner by ensuring that children/young people and employees have an entitlement to safe internet access at all times.

**Significant revisions since the last review:**

- Removed references of internet provider and web filtering referring to NYCC's service to Schools Broadband
- Added reference to GDPR in areas related to publishing of information or images of individuals
- Slight modification to video conferencing wording to account for remote working

## 1 INTRODUCTION

*1.1* King James's School has appointed an e-Safety Coordinator. *This should be the Designated Child Protection Coordinator as the roles overlap.*

*1.2* The KJS e-Safety Policy has been written by the school following guidance from the government and various local authorities. *It has been agreed by the Leadership Team and approved by governors.*

1.3 The e-Safety Policy and its implementation will be reviewed regularly.

**Why the Internet and digital communications are important**

1.4 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

1.5 The Internet is an essential element in 21st century life for education, business and social interaction. It is a powerful tool, which opens up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people have an entitlement to safe internet access at all times.

## 2 TEACHING AND LEARNING

**Internet Use**

2.1 Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

2.2 Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.3 The ICT Department will teach pupils what Internet use is acceptable, and what is not. E- Safety issues will be covered in Year 7, and revisited regularly. The ICT Department will also teach pupils how to use the Internet effectively for research purposes: including skills associated with information location, retrieval and evaluation.

2.4 Staff should guide pupils in on-line activities that will support planned learning outcomes. Pupils engaged in on-line activities should be given clear objectives for Internet use.

**Learning to evaluate Internet content**

2.5 Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of on-line materials is taught in other subject specialisms, not just ICT.

2.6 The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to acknowledge the source of information used.

## 3 MANAGING INFORMATION SYSTEMS

### Maintaining systems security

3.1 The Network Manager will monitor the security of the school information systems. Virus protection will be updated regularly and files held on the school's network will be regularly checked. Advice on security strategies will be sought from NYCC Schools ICT. The network manager will review system capacity regularly.

3.2 Personal data sent over the Internet will use NYCC approved systems.

3.3 Unapproved system utilities and executable files will not be allowed in pupils' work areas, and should not be attached to e-mails.

### Managing e-mail

3.4 The school gives all staff their own email account to use for school business.

3.5 E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.

3.6 Pupils should only use school approved accounts on the school system and only for educational purposes. The ICT Department will teach pupils about the dangers of revealing personal details of themselves or others in e-mail communication; and advise them not to arrange to meet anyone. Pupils must, immediately, tell a teacher if they receive offensive e- mail.

### Management of published content

3.7 The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. Published content should be accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright. Any published content must also comply with any GDPR regulations, with consent being obtained where needed.

3.8 E-mail addresses should be published carefully: to avoid spam harvesting.

### Publishing images

3.9 Permission from parents or carers will be obtained before images of pupils are electronically published in compliance with GDPR regulations.

3.10 Parents will be made aware that we may publish carefully selected images, and that full names will not be used in association with photographs. They may choose not have images of their child published.

### Managing social networking and personal publishing

3.11 Schools Broadband will filter access to social networking sites and newsgroups.

3.12 Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

3.13 Pupils should be advised to be careful about the nature of photographs they put on any public/open social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location eg. house number, street name or school.

3.14 Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

3.15 Teachers' official blogs, wikis, notices and forums should be password protected and run from the school learning platform. Teachers should be advised not to allow pupil access to their personal social network spaces.

**Managing filtering**

3.16 The school subscribes to Schools Broadband Internet Service. The network uses an industry-standard system to filter content and restrict access as appropriate. Additional filtering can be instigated by the school.

3.17 The school will work with the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.

3.18 If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator or Network Manager. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

## 4 USE OF OTHER TECHNOLOGIES

**Video-conferencing**

4.1 Video-conferencing equipment must not be available for pupil use outside of planned lessons based on remote working.

4.2 Video-conferencing should be appropriately supervised at all times. Permission from all participants should be obtained before recording a video-conference lesson.

**Emerging technologies**

4.3 We support the use of appropriate emerging technologies to enhance teaching and learning.

4.4 Mobile phones will not be used for personal purposes during lessons.

## 5 PROTECTION & COMPLAINTS

5.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and General Data Protection Regulations.

**Internet access**

5.2 Parents will be made aware of our internet access, and may choose to have Internet access denied to their child. Pupils must agree to comply with the e-Safety Rules.

5.3 The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

5.4 All staff must read and sign the "Staff Information Systems Code of Conduct‟ before using any school ICT resource.

5.5 The school will endeavour to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Schools Broadband can accept liability for the material accessed, or any consequences resulting from Internet use.

5.6 The school should audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-safety policy is appropriate.

### Handling e-Safety Complaints

5.7 Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to a member of the leadership team. Staff, parents and pupils will need to work together to resolve issues.

5.8 Sanctions for students within the school Discipline Policy may include the following:

- interview/counselling by the head of year
- informing parents or carers
- removal of Internet or computer access for a period

5.9 Discussions will be held with the local Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

### Internet use across the community

5.10 The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

## 6 COMMUNICATION

### Students

6.1 An e-safety module will be included in ICT programmes: covering both school and home use. Instruction in responsible and safe use should precede Internet access.

6.2 E-Safety rules will be posted in rooms with Internet access.

6.3 Pupils will be informed that network and Internet use will be monitored.

### Staff

6.4 All staff will be given the School e-Safety Policy and its application and importance explained. Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

6.5 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

6.6 Staff who manage filtering systems should report any issues to the e-safety coordinator.

### Parents

6.7 Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.

6.8 Internet issues will be handled sensitively, and parents will be advised accordingly.

6.9 Interested parents will be referred to organisations offering e-safety help and advice.