



KING JAMES I ACADEMY

E-Safety Policy

Date adopted by Governors: September 2016

Date of Next Review: September 2017

Introduction

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides awareness for users to enable them to control their online experiences.

The previous Internet Policy has been revised and renamed as the Academy's E-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The Academy's E-Safety Policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

1. End to end E-Safety

- E-Safety at King James I Academy depends on effective practice at a number of levels:
- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies and taught lessons covering e-safety.
- Sound implementation of E-Safety Policy in both administration and curriculum, including secure Academy network design and use.
- The supply of a safe and secure broadband connection from Durham net (IT Services).
- The use of Smart Cache to monitor and filter pupil activity on the internet.

2. E-Safety Policy at King James I Academy

The E-Safety Policy is part of the Academy Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The ICT Coordinator will be responsible for e-safety.
- Our E-Safety Policy has been agreed by the Headteacher and the Senior Leadership Team and approved by Governors.
- The E-Safety Policy and its implementation will be reviewed annually.
- The E-Safety Policy was approved by the Governors in **June 2016**.

3. Teaching and Learning

3.1 *Why Internet use is important?*

- The Internet is an essential element in 21st century life for education, business and social interaction. The Academy has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

3.2 *Internet use will enhance learning*

- The Academy Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3.3 *Students will be taught how to evaluate Internet content*

The Academy should ensure that the use of Internet derived materials by staff and by students complies with copyright law.

Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

All teachers are to advise parents if the content of materials used could cause distress.

4. Managing Internet Access

4.1 *Information system security*

- School ICT systems capacity and security, including for wireless, will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Smart Cache will be maintained up to date.
- The results of misuse collected by Smart cache will be reviewed and the necessary steps be taken with those breaking rules.

4.2 *E-mail*

- All students and staff have a network account and individual email address.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mails sent to an external organisation should be written carefully in the same way as a letter written on Academy headed paper.
- The forwarding of chain letters is not permitted.

4.3 *Published content and the Academy web site*

- The contact details on the web site should be the Academy address, e-mail and telephone number. Staff or students personal information will not be published although pictures of students may be accessible.
- The Headteacher and Graphic Designer, will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.4 *Publishing student's images and work*

- Photographs that include students will be selected carefully and student consent gained before publication.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs.
- All parents and students are asked to sign a consent form, with regard to photographs of students being published on the Academy web site and other Academy publications, when the student joins the Academy.
- Student's work can only be published with the permission of the student and parents.

4.5 *Social networking and personal publishing*

The Academy has a duty of care to provide a safe learning environment for students and staff. The Academy 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 or local authority 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 students, staff and the school through limiting access to personal information:

- The Academy will block/filter access to social networking and gaming sites. (E.g. Bebo, Facebook, Chat rooms, Snapchat, Twitter etc.).
- You Tube will not be available for students but is available for staff.
- Newsgroups will be blocked unless a specific use is approved.

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 discussions on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students must not place personal photos on any social network space.
- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others.
- Sexting - The advice for schools documentation has been shared with key designated safeguarding staff and will be followed if an incident arises.
- The Academy has signed up to take part in the eCadets project, this will allow students and staff to receive support and training in respect to e safety.

4.6 *Managing filtering*

- The Academy will monitor all content when accessing the internet via Smart cache.
- If staff or students discover an unsuitable site, it must be reported to the ICT Network Manager.
- ICT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

4.7 *Managing videoconferencing*

- Videoconferencing will be appropriately supervised for all students.

4.8 *Managing emerging technologies*

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.
- Mobile phones will be switched off during lessons or other formal Academy time unless directed by the teacher to support learning.
- The use of mobile technology to send abusive or inappropriate text messages or email is forbidden as is the videoing or photographing of others without permission.
- iPads will be resourced by the Academy for educational purposes. No student needs to bring an iPad into the Academy as we cannot be held responsible for loss or damage.

4.9 *Protecting personal data*

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

5. Policy Decisions

5.1 Authorising Internet access

- The Academy will maintain a current record of all staff and students who are granted access to school ICT systems.
- Access to the ICT resources and/or the internet will be withdrawn should the system be used inappropriately.

5.2 Assessing risks

- The Academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the Academy, nor the ICT coordinator can accept liability for the material accessed, or any consequences of Internet access.
- The Academy e-safety working group should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the E-Safety Policy is appropriate.

5.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the ICT coordinator or a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures.

5.4 Community use of the Internet

- The Academy will liaise with King James Community and local organisations to establish a common approach to e-safety.

6. Communications Policy

6.1 Introducing the e-safety policy to students

- Students will be informed that network and Internet use will be monitored.
- Students will be informed of The E-Safety policy and of E-Safety through Year 7 ICT and E-safety focus week.

6.2 Staff and the e-Safety policy

- This E-Safety Policy will be stored on the Network in the Staff Shared Area with access for all staff.

- Staff and students should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

6.3 *Enlisting parents' support*

- Parents' attention will be drawn to The Academy E-Safety Policy in newsletters, the Academy brochure and on the Academy website.



King James I Academy

Responsible Internet Use

Rules for Staff and Students

The computer system is owned by the Academy. This Responsible Internet Use statement helps to protect students, staff and the Academy by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- Academy computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made.
- Anonymous messages and chain letters are not permitted.
- The use of Social Media sites such as Snapchat, Facebook, Instagram and Twitter etc. is prohibited on the Academy Network.
- The use of chat rooms is not allowed.
- The Academy ICT systems may not be used for private purposes, unless the Headteacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

The Academy may exercise its right to monitor the use of the Academy'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 Academy'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.

King James I Academy
Responsible Internet Use

Please complete, sign and return to the school secretary

Pupil:

Form:

Pupil's Agreement

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

Signed:

Date:

Parent's Consent for Internet Access

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

Signed:

Date:

Please print name:

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the Academy website. I also agree that photographs that include my son/daughter may be published subject to the Academy rules that photographs will not clearly identify individuals and that full names will not be used.

Signed:

Date:

This consent form is based, with permission, on the Internet Policy of the
Irish National Centre for Technology in Education.
