King Richard School

E-Safety Policy

Table of Contents

E-Safety Policy

Written by	United Learning/James Webb	Job Title	
Owned by	United Learning/James Webb	Job Title	
Applies to	Staff ☐	Students	☐
	Parents ☐	Governors	☐
Reviewed on	April 2018		
To be reviewed on	April 2019		
Version	1		

Introduction

The e-safety policy is a key element of the Technology Policy as it is about the safe and responsible and ethical use of online technologies. It covers accessing online resources through computers, tablets, smart phones and any other internet enabled device safely and effectively. In conjunction with the Social Media policy, it includes new social media tools and other emerging trends. It should cover a range of issues and not condemn the use of tools but rather address how to use them safely. This should include how to comment appropriately in many different forums, including social media and not being just a bystander. An essential part of this is how to report concerns, online and offline.

- Safeguarding and promoting the welfare of students is embedded into the culture of King Richard School and its everyday practice and procedures. All staff have a responsibility to support E-safe practices in school and all students need to understand their responsibilities in the event of deliberate attempts to breach E-safety protocols.

- Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with King Richard School's Anti-Bullying and Behaviour Policy.

- Complaints related to child protection will be dealt with in accordance with King Richard School's Safeguarding Policy. [Issues/ concerns MUST always be reported to the designated Child Protection Officer]

Key Personnel

JAMES WEBB ASSISTANT HEADTEACHER

Areas of risk

Child Protection	Children are exploited by sex offenders Children upload inappropriate content online Children publish personal information which identifies them either overtly or covertly (location metadata in images or messages) Staff do not understand the technology and under (or over) estimate the risk
Staff Protection	Staff post comments or images which compromise their professional integrity Staff lack of understanding of new online tools puts them at risk.

OFSTED Inspection	Lack of understanding of the e-safety policy by staff, students or governors can prevent a school from achieving an excellent or outstanding inspection judgement.

Scope

This e-safety policy should be read in conjunction with other policies with the over-arching Technologies Policy but with particular reference to the Mobile Devices Policy, Social Media Policy and Internet Filtering Policy

Policy Statements

Communicating with children electronically

*Only electronic communication between staff and students u*sing online services and sites provided by United Learning are permitted.

Social Networking and Chat Rooms

- King Richard School will control access to social networking sites and educate students in their safe use.
- Students will be taught the importance of personal safety when using social networking sites and chat rooms.
- Students will not be allowed to access public or unregulated chat rooms.
- Students will be advised to use appropriate nick names and avatars when using social networking sites. Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

Teaching and Learning:

- Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of students.
- Students at King Richard School will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students at King Richard School will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of search engines and encouraged to question the validity.
- Students at King Richard School will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- Students at King Richard School will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.
- E-Safety rules (Email, web searching, reporting problems etc) displayed in all IT rooms.•

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Letters, newsletters, web site*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications eg www.swgfl.org.uk* www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (

Education – The Wider Community

The school / academy will provide opportunities for local community groups / members of the community to gain from the school's / academy's e-safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and e-safety*
- *E-Safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school / academy website will provide e-safety information for the wider community*
- *Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision*

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.** *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.**
- *The E-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.*

Training – Governors / Directors

Governors / Directors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

E-safety Information

- **Internal resources**
  School Website, **Internal File Server**
- **External resources**
  https://www.kingrichardschool.net

Reporting Procedures

Reporting Procedures – See Filtering Policy for more information:

- Internal reporting on students and staff is carried out using internet filtering and key logging software to identify any concerns inline with our Safeguarding and Child Protection policies.
- Reports will be monitored on a regular basis and any concerns raised with the DSL, who will in accordance with appropriate school polices pass the information on to the relevant person. Please refer to the Filtering & Monitory Policy for details.
- External parties can also report any concerns via the school's website or the Child **Exploitation & Online Protection (CEOP) "Report Abuse" button at www.ceop.police.uk.**

Photographic, Video and Audio Technology

♣ Staff may use school owned photographic or video technology to support school trips and appropriate curriculum activities.

♣ King Richard School will maintain a record of students whose parents/carers have specifically requested that video and photographic images are not made of them.

Assessing and Managing Risks

Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

- In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet account, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Multi Academy Trust can accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

Maintaining ICT Security (including password security)

- Personal data sent over the network will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in student' work areas or attached to e-mails.
- Password security is of the utmost importance and must be maintained at all times. Adults and students will be reminded never to disclose their passwords. Concerns reported to the Network Manager.
- Users shall treat as confidential any information which may become available to them through the use of such facilities and which is not on the face of it intended for unrestricted dissemination; such information shall not be copied, modified, disseminated, or used either in whole or in part without the permission of the person or body entitled to give it
- No user may use ICT facilities to hold or process data relating to a living individual save in accordance with the provisions of current data protection legislation

Appendix D – e-Safety Reporting Log

School: *King Richard School*

Date	Time	Incident	Action Taken		Incident Reported by	Signature
			What?	By Whom?		