

Kingsdown Secondary School E-safety Policy

School E-safety

1. Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, Acceptable Computer Use, Anti-Bullying and for Safeguarding.

- Our e-Safety Policy has been written by the school. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: ...Yusif Assim
- It was approved by the Governors on:
- Our E-safety policy relates to both existing and emerging technologies: see Appendix 1

2 Teaching and learning

All Internet use by staff and pupils is governed by the school's Acceptable Internet Use Agreement

2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils need to be aware of the dangers in cyberspace and taught how to use the Internet safely.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Pupils using the Internet

- The school Internet access is designed for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable, in accordance with the school's Acceptable Internet Use Agreement, and given clear objectives for Internet use.
- Pupils will be taught how to use the Internet safely.

3 Managing Internet Access

3.1 Information system security

- School ICT systems' capacity and security will be reviewed regularly.
- Virus protection will be updated regularly by the School based technician.
- Internet access will be filtered by more robust software such as Bloxx to give more protection and security to users.
- Security strategies will be discussed with the Head Teacher, Principal of school, school base technician and the school external network support.

3.2 E-mail

- Pupils may use e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication.
- E-mail sent by pupils to an external organisation should be written carefully and authorised by a member of staff before sending, in the same way as a letter written on school headed paper.

3.3 Published content and the school web site

- The contact details on the Web site should be the school address, webmaster and school e-mail, fax and telephone number. Staff or pupils' personal information will not be published.
- The headteacher and the director of school has overall editorial responsibility and will ensure that content is accurate and appropriate.

3.4 Publishing pupils' images and work on the school website

- Photographs that include pupils and any published work will not enable individual pupils to be clearly identified unless permission has been given by parents.
- Pupils' 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 pupils are published on the school Web site.

3.5 Social networking and personal publishing

- The school network technician controls access to social networking, messaging and blogging sites. All have been blocked unless requested by staff and use for educational purpose.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Pupils and parents will be advised that the use of some social network spaces outside school is inappropriate for certain aged groups(11-16yrs).

3.6 Managing filtering

- The network technician controls all internet filtering.
- If staff or pupils discover an unsuitable site which is not filtered, it must be reported to the network technician.
- The School use Bloxx filtering system to manage their computer systems.

3.8 Other Communications technologies

- Emerging technologies (see Appendix 1) will be examined for their educational benefit and a risk assessment will be carried out before any use in school is allowed.
- Mobile phones or other hand held communication or games devices are not used during lessons or formal school time. Any such devices brought into school will be handed to the class teacher or the administrator at the beginning of the day and can only be claimed back at the end of the day. Any such devices found in a pupil's possession during the day will be confiscated and returned to the pupil's carer(s).Such devices can only be use for educational purposes under the instructions of a teacher or instructor.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998(see Data Protection Policy)

4 Policy Decisions

4.1 Authorising Internet access

- All staff must read and sign the Staff e-safety Code of Conduct (Appendix) before using any school ICT resource.
- The school will keep a record of any incident resulting in a pupil's access being withdrawn.
- Pupils will be allowed to browse the Internet appropriately and only under the supervision of staff.

4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- Neither the school nor the management can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

4.3 Handling e-safety complaints or incidents

- Complaints of Internet misuse will be dealt with by the Head of School and ICT co-ordinator. Any complaint about staff misuse must be referred to the Head of School. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police if any e-safety issue with legal implications arises.
- Cyberbullying or other abuse between our pupils taking place offsite can seriously affect relationships in school. Any cyber bullying incident which has such an effect will be dealt with in accordance with the school's Ant-Bullying policy. (See Appendix 2)

4.4 Community use of the Internet

- Any community user of the school's ICT facilities will be made aware of this policy and our Acceptable Internet Use policy and their agreement to abide by them required before such use is granted.

5 Communications Policy

5.1 Introducing the e-safety policy to pupils

- Network use, including e-safety, rules will be posted in all areas with networked computers in accordance with the school's Acceptable Internet Use Policy.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils should be taught what to do if they access material they are uncomfortable with.

5.2 Staff and the e-Safety policy

- All staff will be made aware of the School e-Safety Policy and its importance explained.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user, in accordance with the school's Acceptable Computer Use and ICT policies.
- Staff must adhere to the Code of Conduct regarding the use of mobile phones and other personal technology in school and on school business.

5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.

Documents used and consulted in preparation of this policy:

WSCB e-safety Booklet

DSCF Cyber bullying – Safe to Learn: Embedding Anti-Bullying Work in Schools

NGFL Acceptable Use Policy for Adult Users

BECTA Signposts to Safety: Teaching E-Safety.

Appendix 1: E-technologies

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

Internet	Our approach in school
The web	filtered by our own web filtering (Bloxx), site blacklist
e-mail	Staff monitored accounts,
Instant messaging (e.g. MSN)	all blocked except use as part of delivering the curriculum
Blogs	moderated by teachers
Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)	uploaded by school network engineer
Social networking sites such as MySpace, Bebo, Piczo, Facebook	all blocked in school except use as part of delivering the curriculum
Video broadcasting sites such as YouTube	all blocked in school except allowed by staff for specific purpose.
Chat Rooms	all blocked in school except use as part of delivering the curriculum
Gaming Sites	blocked in school wherever possible except allowed by staff or needed for learning purposes
Music download sites	blocked in school wherever possible
wikis	moderated by teacher/network technician
Non-Internet	
Mobile phones with camera and video functionality	all banned in school except use as part of delivering the curriculum
Mobile technology (e.g. games consoles) that are 'internet ready'.	banned, unusable in school except use as part of delivering the curriculum
Smart phones with e-mail, web functionality and cut down 'Office' applications.	banned in school except use as part of delivering the curriculum

Appendix 2

What to do if a cyber bullying incident occurs:

Based on "Cyber bullying – Safe to Learn: Embedding Antibullying work in schools" DCSF-00658-2007

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

1. Advise the child not to respond to the message
2. Refer to relevant policies including e-safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
3. Secure and preserve any evidence
4. Inform the sender's e-mail service provider
5. Notify parents of the children involved
6. Consider delivering a parent workshop for the school community
7. Consider informing the police depending on the severity or repetitious nature of offence
8. Inform the School Safeguarding officer/ LA e-safety officer

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform the site administrators and / or ISP and request the comments be removed if the site is administered externally
2. Secure and preserve any evidence
3. Send all the evidence to CEOP(Child Exploitation and Online Protection Centre) at www.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform police as appropriate
5. Inform School Safeguarding officer/ LA e-safety officer

The school may wish to consider delivering a parent workshop for the school community

Children and staff should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear, even if they have initially responded to the abuse.

This policy will be reviewed again in January 2016