# E-Safety

| | | | |
|---|---|---|---|
| Date of review | March 2019 | Review period | 2 yearly |
| Date of next review | March 2021 | Author | N Burrell/L Pippin |
| Type of policy | Statutory | Approval | Governing Board |

E-Safety encompasses the use of new technologies, internet and electronic communications, publishing and the appropriate use of personal data. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

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

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

## The Core e-Safety Policy

This core e-safety policy provides the essential basic coverage and has been based upon the Kent County Council's Children, Families and Education Directorate.

## End to End e-Safety

E-Safety 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.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Durham.net and Smooth Wall filtering.
- National Education Network standards and specifications.

E-Safety Audit

This quick audit will help the Senior Leadership Team (SLT) assess whether the basics of e-Safety are in place.

| | |
|---|---|
| The school has an e-Safety Policy that complies with CFE guidance. | Y/N |
| Date of latest update: 11.07.16 | |
| The Policy was agreed by governors on: .11.07.16 | |
| The Policy is available for staff in school policy file on portal | |
| And for parents at school website | |
| The Designated Child Protection officer – Mrs L Pippin | |
| The e-Safety Coordinator is Mrs L Pippin | |
| | |
| Has LEA training been considered/implemented? | /Y |
| All staff sign an Acceptable ICT Use Agreement on appointment. | Y/ |
| Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement. | Y |
| Rules for Responsible Use have been set for students: | Y |
| E-safety Rules are displayed in all rooms with computers. | Y |
| Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access. | Y |
| The school filtering policy has been approved by SLT. | Y |
| An ICT security audit has been initiated by SLT, possibly using external expertise. | Y |
| School personal data is collected, stored and used according to the principles of the Data Protection Act. | Y |
| Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT. | Y |
| Named staff have had eSafety training | Y |

**School e-safety policy.**

**2.1 Writing and reviewing the e-safety policy**

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

- The school will appoint an e-Safety coordinator.
- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy will be reviewed annually.
- The e-Safety Policy was revised by: Boldon School S.L.T.

**2.2.1 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 students with quality Internet access as part of their learning experience. The school however reserves the right to limit internet usage for al persons not adhering to e-safety guidelines.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

**2.2.3 Internet use will enhance learning**

- The school Internet access 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

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

- Internet derived materials by staff and by students must comply with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**Currently our Ranger and E-Safe systems will be used to monitor and control the use of school communication systems.**

**2.3.1 Information system security**

- The school's ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with Civica, the Local Authority and NGFL.
- It is not recommended that anyone should remove data from school either by using a device or by taking personal information home in paper form unless absolutely necessary. Do not leave any device or paperwork in your car or elsewhere (see the Data Protection Policy which explains what to do in the event of a Data Breach). If you do need to remove data from school via a data pen or other means you **MUST** ensure it is encrypted to prevent unauthorised access if lost or stolen. Please see the IT Technician or Administration Leader for instructions on encrypting your device.

**2.3.2 E-mail and internet access**

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail or accidentally access inappropriate sites. The teacher should then log this with the E-safety officer for investigation.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.
- Staff E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- **Transferring Personal Data** - Any transfer of personal data must be done securely:

  Email communication is not always secure and sending personal data via external email should be avoided. You MUST use an Email encryption service for any emails sent which include personal data. Egress switch is recommended, a service which is also being rolled out across the LEA. Should your recipient not have Egress they will be invited to register when they receive your email. It is a free service, please use the following link to sign up: - https://switch.egress.com/ui/registration/accountcreate.aspx

  Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

Personal email accounts should not be used to send or receive personal data for work purpose.

**2.3.3 Published content and the school web site**

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or students personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

**2.3.4 Publishing students' images and work**

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- Work can only be published with the permission of the student and parents.

**2.3.5 Social networking and personal publishing**

- School will block/filter access to social networking sites as appropriate with the possible exception of school discussion groups on the school's VLE.
- Staff should not access social networking sites in school time and must not engage students or accept students into groups/friends on social networking sites at any time.
- Staff should bear in mind that professional standards must be maintained even when privately posting images and comments on social network sites. Comments on such sites should not refer to their work life.
- Newsgroups will be blocked unless a specific use is approved.
- 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 should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

**2.3.6 Managing filtering**

- The school will work in partnership with Civica, the LA, DfES and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager (Civica).
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will use E-Safe software to monitor all persons logged onto school systems and reports will be sent to the named E-safety Officer (Ian Noble; Deputy Head Teacher)

### 2.3.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students must ask permission from the supervising teacher before making or answering a video-conference call.
- Video-conferencing will be appropriately supervised for the students' age.

### 2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time and should be switched off unless permission is given by a member of staff.
- The use of camera phones to take pictures is **not permitted.** If photographs related to school business need to be taken then a school camera should be used and the images downloaded to the appropriate area on the network. The images should then be deleted from the camera.
- Staff should not use their mobile phone for school business and should not give their own numbers to parents or students.
- If it is necessary to communicate with students, when on a visit for example, then the school mobile phones should be used and their numbers given to students and parents
- The sending of abusive or inappropriate text messages is forbidden.

### 2.3.9 Protecting personal data

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

### 2.4.1 Authorising Internet access

- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.
- Students must apply for Internet access individually by agreeing to comply with the Responsible Use statement for use of school systems
- Parents will be asked to sign and return a consent form.

### 2.4.2 Assessing risks

- The school 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

### 2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher or E-safety officer.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer and other relevant bodies to establish procedures for handling potentially illegal issues.

**2.4.4 Community use of the Internet**

- The school will liaise with local organisations to establish a common approach to e-safety and anyone using the school's system must sign the acceptable use policy before access is granted.

**2.5 Communications Policy**

**2.5.1 Introducing the e-safety policy to students**

- e-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.

**2.5.2 Staff and the e-Safety policy**

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff 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.

**2.5.3 Enlisting parents' support**

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

**NOTE – THE FACILITIES MANAGEMENT ON SITE IS MITIE AND THEY HAVE THEIR OWN ITT SECURITY POLICY IN PLACE WHICH CAN BE PROVIDED IF REQUIRED**

# BOLDON SCHOOL

## E-SAFETY RULES

These e-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible or inappropriate use **may** result in the loss of network or Internet access.
- No files or programs may be stored or accessed on the network from a data pen or other storage device without the permission of a member of staff.
- Network access must be made via the user's authorised account and password, **which must not be given to any other person.**
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised or inappropriate use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

# BOLDON SCHOOL

## E-SAFETY AGREEMENT FOR STUDENTS & PARENTS

***All students use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both students and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed. The Rules are displayed in all networked rooms within school and can also be accessed on the school website.***

***Student:*** _____ ***Reg. Group:*** _____

**Student's Agreement**

- I have read and I understand the school e-Safety Rules.
- I will only use the computer, network, mobile phones, Internet access and other new technologies with the permission of a member of staff and in a responsible way at all times.
- I know that network and Internet access may be monitored.

***Signed (student):*** _____ ***Date:*** _____

**Parent's Consent for Web Publication of Work and Photographs**

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by student names.

***Signed:***_____ ***Date:***_____

**Parent's Consent for school information systems and Internet Access.**

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

***Signed:*** _____ ***Date:*** _____

***Please print name:*** _____

## BOLDON SCHOOL – PLEASE COMPLETE & RETURN TO THE SCHOOL OFFICE

## STAFF INFORMATION SYSTEMS CODE OF CONDUCT

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems (including laptop computers) are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional rôle.
- I understand that school information systems may not be used for private purposes, without specific permission from the Head Teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and **I will not disclose any password or security information** to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with students are compatible with my professional rôle.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

**I have read, understood and agree with the Information Systems Code of Conduct.**

Signed: …… Capitals: …… Date: ……

Accepted for school: ……. Capitals: …….

## BOLDON SCHOOL – PLEASE COMPLETE & RETURN TO THE SCHOOL OFFICE

## VISITOR INFORMATION SYSTEMS CODE OF CONDUCT

To ensure that visitors are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Visitors should consult the school's e-safety policy for further information and clarification.

- The information systems (including laptop computers) are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional rôle.
- I understand that school information systems may not be used for private purposes, without specific permission from the Head Teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and **I will not disclose any password or security information** to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with students are compatible with my professional rôle.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

**I have read, understood and agree with the Information Systems Code of Conduct.**

Signed: …….…… Name in Capitals: ……..……Date: ……..……

Accepted for school: ……..……. Name in Capitals: ……..……..

# BOLDON SCHOOL

## Screening Tool

This screening tool can be used to assist decision making in dealing with incidents of computer or e-communications misuse within school. It can be used to inform initial action but is not a substitute for a thorough risk assessment / investigation.

This should be used alongside the e-Safety flow chart and incidents of misuse matrix.

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, please contact a member of the Children's Safeguard Service.

**Type of incident**

Sexual ☐
Bullying ☐
Violence ☐
Incitement ☐
Financial ☐
Grooming ☐
Other ☐

**How was the incident discovered?**

Self reported ☐
Reported by 3rd party (friends or parents) ☐
Reported by Teacher ☐
Other (e.g. Police or Internet Watch foundation) ☐

**What was their response to the incident?**

Unconcerned ☐
Curious ☐
Distressed ☐
Frightened ☐
Secretive ☐
Other ☐

**What did the incident refer to?**
Answer the key questions relating to the particular incident

Child as Victim:

Content

1. What was the type of content? (Sexual, violence, racial, other)
2. Did anyone else see it?
3. Have they told anyone else about it?

**Publishing**

1. Is the child identifiable?
2. Can their location be traced/
3. Is text or image potentially indecent or illegal?

**Bullying**

1. What was the type of bullying? (sexual, violent, physical, group)
2. Were information or images published of the child?
   (If yes, refer back to publishing section for more questions to ask)

**Predation / Grooming**

1. Assess the extent of the contact
   - One off conversation
   - Regular conversation
   - Regular conversation using inappropriate or sexualised
   - language or threats
   - Attempts to breakaway
   - Offline meeting arranged
   - Offline meeting occurred
     (Consider if an offence has occurred)

2. Are the parents aware?
3. When did the incident occur?

**Request for information**

1. Did the child give out any personal information?

**<u>Child as Instigator</u>:**

**Content**

Refer to 'Child as Victim' questions on content
Refer to AIM project matrix to assess the child's response to the content

**Incitement**

1. Was the child secretive about the site?
2. Did the child access the site in an isolated place?
3. Did they understand the risks of accessing this site?

4. Was their response to the site?
   - Healthy (e.g. using for research)
   - Problematic (looking for advice or guidance)
   - Harmful (relying on site for tips, using site to communicate with likeminded individuals, the site is reinforcing /minimising potentially harmful behaviours e.g. self-harm, pro anorexia sites

**Send/Publishing**

1. Has an offence taken place?
   (Refer to glossary for information on what constitutes an offence)
2. Were others put at risk e.g. their image / information was sent / published
3. Was this an isolated incident or persistent?
4. Did the instigatator have empathy for the victim?

**Interception of communications / Hacking**

1. Have they placed themselves or others at risk?
2. Has personal or financial information been stolen?
   (If yes, this constitutes a criminal offence and advice should be sought from the police)
3. Has illegal content been accessed and sent to other's computers?

Once you have gathered the appropriate information, assess the effect of the incident on the child and identify how the child can be best supported. This may be either in school (using existing policies and resources to support children) or in certain circumstances with external help.

**Staff misuse**

Did the member of staff misuse the school's internal email system?

Did the member of staff communicate with a young person inappropriately e.g. via text message, multimedia images.

Consider the extent of the communication

- One off conversation
- Regular conversation
- Regular conversation using inappropriate or sexualised language or threats
- Attempts to breakaway
- Offline meeting arranged
- Offline meeting occurred

Did the member of staff access inappropriate/ illegal material within school?

Did the member of staff access inappropriate/ illegal material using school equipment?

Did the member of staff access inappropriate/ illegal material using their own equipment?

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, please contact the child protection officer before taking any other action.

**Glossary**

Many young people use the internet regularly without being aware that some of the activities they take part in using the internet are potentially illegal.

The 2003 Sexual offences Act has introduced new offences of Grooming and raised the age for making/distributing indecent images of children to 18.

Offences regarding racial hatred are covered by the Public Order Act 1986 although there is currently a new Racial and religious Hatred Bill going through parliament.

Bullying etc could be an offence under the Malicious Communications Act 1988 or Telecommunication Act 1984

Other potential offences may include Fraud (e.g. using false identities) or infringements of the Data Protection Act.

**List of offences:**

**Sexual Offences Act 2003**

Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18.
(NB to view an indecent image on your computer means that you have made a digital image.)

Causing a child under 16 to watch a Sexual Act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.

Abuse of positions of trust. Staff need to be aware that it is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Applies to teachers, social workers, health professionals, connexions Pas)

N.B. the school should have a copy of 'Children & Families: Safer from Sexual Crime' document as part of the child protection pack.
Alternatively information about the 2003 Sexual Offences Act can be found at www.teachernet.gov.uk

**Public Order Act 1986** – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

**Telecommunications Act 1984** – Offence to send by public telecommunications network any offensive, indecent, obscene or menacing messages that cause annoyance/inconvenience/needless anxiety.

**Malicious Communications Act 1988** – offence to send letter or article which includes indecent, grossly offensive, threatening or false information with the intent of causing anxiety/stress to the recipient.

**Protection from Harassment Act 1997 –**

Section 1 - A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

Section 4 - A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

**Response to an incident of concern**

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

Any e-Safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to e-safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to students and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Co-ordinator, the e-Safety Officer or the Police Liaison Officer.

**What does electronic communication include?**

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research**: web sites, search engines and Web browsers
- **Mobile Phones and personal digital assistants** (PDAs)
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**

**What are the risks?**

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information / images

- Identity theft
- Hacking and security breaches

**How do we respond?**

The flowchart on the next page is taken from the Kent C.C. material and illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Children's Safeguards service has provided supporting documents to assist schools when responding to incidents.

Please see the Children's Safeguards Service website:

http://www.clusterweb.org.uk?safeguards

Response to an Incident of Concern

The Screening Tool is available in the policy and on the Children's Safeguards Service site listed above.