Burradon Community Primary School

2020 E-Safety Policy

Updated September 2020
Mrs E Watson

Contents

Schools and Settings e-Safety Policy

2.1 Who will write and review the policy?
2.2 Teaching and Learning
2.2.1 Why is Internet use important?
2.2.2 How does Internet use benefit education?
2.2.3 How can Internet use enhance learning?
2.2.4 How will pupils learn how to evaluate content?
2.3 Managing Information Services
2.3.1 How will information systems security be maintained?
2.3.2 How will email be managed?
2.3.3 How will published content be managed?
2.3.4 Can pupil images and work be published?
2.3.5 How will social networking and personal publishing be managed?
2.3.6 How will filtering be managed?
2.3.7 How will videoconferencing be managed?
2.3.8 How can emerging technologies be managed?
2.3.9 How should personal data be protected?
2.4 Policy Decisions
2.4.1 How will Internet access be authorised?
2.4.2 How will risks be assessed?
2.4.3 How will complaints be handled?
2.4.4 How should the Internet be used across the community?
2.4.5 How will Cyberbullying be managed?
2.4.6 How will Learning Platforms be managed?
2.5 Communications Policy
2.5.1 How will the policy be introduced to pupils?
2.5.2 How will the policy be discussed with staff?
2.5.3 How will parents’ support be enlisted?
3.0 e-Safety Audit, Contacts and References

2.0 School e–Safety Policy

2.1 Who will write and review the policy?

- The school has an e-Safety Coordinator – Elaine Watson (E-Safety co-ordinator/deputy head). The e-Safety Policy and its implementation will be reviewed annually.
- Our e-Safety Policy has been written by the school. It has been agreed by the Senior Leadership Team, staff and approved by governors. A copy of the policy is available for parents in the front office.

2.2 Teaching and learning

Teaching online safety is not optional – the school is required to put in place strengthened measures to protect children from harm online, including cyber bullying.

2.2.1 Why is Internet use important?

Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is a part of everyday 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. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- E-Safety is part of the Computing 2014 Curriculum at KS1 and KS2 and all pupils must be taught the importance of keeping safe online and how to use technology responsibly, safely and securely.

2.2.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- access to learning wherever and whenever convenient.

2.2.3 How can Internet use enhance learning?

The school's Internet access will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

2.2.4 How will pupils learn how to evaluate Internet content?

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of online materials is a part of teaching/learning in every subject.

2.3 Managing Information Systems

2.3.1 How will information systems security be maintained?

The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly.

- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.

2.3.2 How will email be managed?

- Pupils may only use approved email accounts (Gmail through Airhead).
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole class or group email addresses will be used in primary schools for communication outside of the school.
- KS2 pupils will use their Gmail e-mail at school for communication outside of school. Staff and ICT coordinator will be responsible alongside the LA in monitoring e-mails.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- Schools may have a dedicated email for reporting wellbeing and pastoral issues and this inbox must be approved and monitored by members of Senior Leadership Team.
- Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours or for professional purposes.

2.3.3 How will published content be managed?

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

- Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT'.
- The head teacher and deputy head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

2.3.4 Can pupil's images or work be published?

- Images that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

See appendix 1

2.3.5 How will social networking, social media and personal publishing be managed?

The school will control access to social media and social networking sites.

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 email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils should be advised not to place personal photos on any 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 student or his/her location.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Staff should be advised not to run social network spaces for pupil use on a personal basis.
- If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.
- 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 by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

2.3.6 How will filtering be managed?

The school will work with Becta and the Local Authority ICT consultants to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator. (see appendix 2)

The school's broadband access will include filtering appropriate to the age and maturity of pupils.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

2.3.7 How will videoconferencing be managed?

- Videoconferencing should be supervised appropriately for the pupils' age.
- Parents and carers should agree for their children to take part in videoconferences, probably in the annual return.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

2.3.8 How can emerging technologies be managed?

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. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Staff and visitors using mobile devices must ensure that they are connected to the school's website and not their own personal 4/5G.

2.3.9 How should personal data be protected?

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

2.4 Policy Decisions

2.4.1 How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the 'Staff Acceptable user policy see appendix 3) before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.

  Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is available).

2.4.2 How will risks be assessed?

The school will take all reasonable precautions 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. The school nor LA can accept liability for the material accessed, or any consequences resulting from Internet use.

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.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

2.4.3 How will e–Safety complaints be handled?

Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.

Any complaint about staff misuse must be referred to the headteacher.

All e-Safety complaints and incidents will be recorded by the school — including any actions taken.

- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

2.4.4 How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-Safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

- Esafety information for parents/carers and pupils to be available on school website.

2.4.5 How will Cyberbullying be managed?

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying and our cyberbullying policy.

There will be clear procedures in place to support anyone affected by Cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying (refer to cyber bullying policy) may include:
  - The bully will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content.
  - Internet access may be suspended at school for the user for a period of time.
  - Parent/carers may be informed.
  - The Police will be contacted if a criminal offence is suspected.

2.4.6 How will Learning Platforms and learning environments be managed?

SLT and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.

Pupils/staff will be advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have access to the LP.

All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

- Any concerns with content may be recorded and dealt with in the following ways:

  a) The user will be asked to remove any material deemed to be inappropriate or offensive.

  b) The material will be removed by the site administrator if the user does not comply.

  c) Access to the LP for the user may be suspended.

  d) The user will need to discuss the issues with a member of SLT before reinstatement. e) A pupil's parent/carer may be informed.

- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

2.5 Communication Policy

2.5.1 How will the policy be introduced to pupils?

All users will be informed that network and Internet use will be monitored.

An E-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.

- Pupil instruction in responsible and safe use should precede Internet access.
- An e-Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- e-Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.
- Use of outside agencies to support teaching and learning for pupils and teachers of e-safety.

2.5.2 How will the policy be discussed with staff?

The e-Safety Policy will be formally provided to and discussed with all members of staff.

To protect all staff and pupils, the school will implement Acceptable Use Policies. (Attached to policy appendix 3)

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 the Senior Leadership Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

2.5.3 How will parents' support be enlisted?

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

- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e-Safety at other attended events e.g. parent evenings, sports days.
- Parents will be requested to sign an e-Safety/internet agreement as part of the Home School Agreement.
- Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in section "e-Safety Contacts and References." (Appendix 4)

Appendices

Appendix 1

1. Children's Safeguards site, "use of photographic images of children" ***www. kenttrustweb.org.uk?safeguards*** (Policy and Guidance section)

Appendix 2

E-Safety Incident Report Form

Date	Incident	Action	Reported by

Appendix 3

Acceptable User Policy (Updated July 2020)

The aim of this Acceptable Use Policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet and email use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

It is envisaged that the AUP will be revised annually. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

Updated September 2020

by Elaine Watson (E-Safety Lead)

School's Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Internet sessions will always be supervised by a teacher, TA or ICT Techno buddy (lunchtimes rules and restrictions apply).
- Filtering systems are used by our ISP, (North Tyneside), in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor pupils' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software is present on all machines and is updated and checked automatically on a daily basis.
- The use of personal memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

- All staff have password protected memory sticks for sensitive data and school photographs.

World Wide Web

- School staff and pupils will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- School staff and pupils will pupils report accidental accessing of inappropriate materials in accordance with school procedures.
- Pupils will use the Internet for educational purposes only.
- Pupils will not copy information into work without acknowledging the source (plagiarism and copyright infringement).
- Pupils will **NEVER** disclose or publicise personal information.
- Downloading materials or images not relevant to class work and homework is in direct breach of the school's acceptable use policy.
- School staff and pupils will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email

- School staff and pupils will use approved email accounts.
- School staff and pupils will not send or receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
- Pupils will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Pupils will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Pupils will note that sending and receiving email attachments is subject to permission from their teacher.

Internet Chat

- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication forums that have been approved by the school, e.g. within the Learning Platform(Airhead).
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat will be forbidden.

School Website

- Pupils will be given the opportunity to publish projects, artwork or school work into, Seesaw or school website in accordance with clear policies and approval processes regarding the content that can be uploaded – this will be facilitated by the class teacher or nominated school adult.

- The school's website, Twitter and Seesaw will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publication of pupil work will be co-ordinated by school staff.
- Parental permission will be sought at the beginning of child starting our school. Class teacher to ensure any new pupils' parents/carers complete permission form.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the first name and last name of individuals in a photograph.
- The school will ensure that the image files are appropriately named – will not use pupils' names in image files if published on the web.
- Pupils will continue to own the copyright on any work published.

Personal Devices

Pupils using their own technology in school, such as leaving a mobile phone turned on to send nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy. Pupils are not permitted to have Mobile phones in school. If parent/carer requests for a specific reason the mobile phone will be switched of and sent to the school office for safe storing.

Visitors and staff must ensure that their mobile devices being used in school are connected to the school's Wifi and to personal 4/5G. The password for the Wifi is available from the school office, Computing lead and the e-safety lead.

School ipads

- Pupils to be taught how to keep themselves safe on ipads. (See e-safety policy.)
- Children to be supervised when using ipads.
- Pupils are not allowed to download apps onto school ipads.

Support Structures

The school will inform pupils and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Acceptable Use Policy: Adults working in school

All adults working with ICT equipment in Burradon Community Primary School must ensure that they have read and agree to abide by the User Policy.

Personal use:

Do not give anyone access to your login name or password.

Do not open other people's files without express permission. Do not corrupt, interfere with or destroy any other user's information.

Do not release personal details including phone numbers, fax numbers or personal e-mail addresses of any colleague or pupil over the Internet.

Do not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used.

Do not attempt to visit sites which might be considered inappropriate. All sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

Use of school Internet access for business, profit, advertising or political purposes is strictly forbidden.

Users should log out and close their browser when their session has finished.

Visitors and staff must ensure that their mobile devices being used in school are connected to the school's Wifi and to personal 4/5G. The password for the Wi-Fi is available from the school office, Computing lead and the E-safety lead.

Personal E-mail:

Follow school guidelines contained in the ICT policy for the use of e-mail.

Observe *netiquette* on all occasions. E-mail should not be considered a private medium of communication.

Do not include offensive or abusive language in your messages or any language which could be considered defamatory, obscene, menacing or illegal. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority. You should be aware that school e-mail can be monitored.

Make sure nothing in the messages could be interpreted as libellous.

Do not send any message which is likely to cause annoyance, inconvenience or needless anxiety.

Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.

When using the Internet, Learning Platform (Airhead) or e-mail with children

Remind children of the rules for using the Internet, the Learning Platform or e-mail.

Check before publishing children's work; make sure that you have parental permission.

Ensure children cannot be identified from photographs on the website, Twitter and Website.

Report any breaches of the school's Internet policy to the designated person.

Covid-19 Addendum

- Online teaching should follow the same principles as teaching in school as set out in our ICT Policy.
- Whilst staff are interacting with children away from the school online, they must continue to adhere to the Professional Conduct of Staff, Safe Working Practice Policy, ICT and E-Safety Policy and any other policies, protocols, professional standards and statutory guidance applicable to their role.
- Staff should use parents' or carers' email addresses or phone numbers from the school office management information system (SIMs).
- Staff should use their school email accounts to communicate via email or through Seesaw, never use personal accounts.
- In light of our change in practice due to COVID19, it may be necessary for staff to use their personal mobile phones to communicate with students, parents and carers. Where this is deemed necessary, this must be agreed by a member of the Leadership Team. Where applicable, staff should make sure any phone calls from a personal device are made from a blocked number, so personal contact details are not visible. Keying 141 before the phone number will block your caller ID on the call you're making.
- If staff members are accessing families' contact details at home, ensure they comply with the Data Protection Act 2018.

Reporting Concerns

Communicating online may allow you a view into a young person's world that you would not have seen before (and would maybe not have had the opportunity to without this crisis). This may also generate some safeguarding concerns for that young person. It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Any concerns must be recorded and a Designated Safeguarding Lead (DSL) must be informed immediately**.**

Staff /Adult Form

Please read the attached school Acceptable Use Policy sign and return this permission form to the Headteacher.

Name: ______________________

Role: ______________________

I agree to follow the school's Acceptable Use Policy on the use of the Internet and computers. I will use the Internet in a responsible way and obey all the rules explained to me by the school.

Signature: ____ Date:

In accordance with GDPR 2018 (Data protection) please refer to the policy on our school website using the following hyperlink for information on how we collect, control, process and protect data.

Please note : we share some data with the Local Authority, DfE and outside agencies as defined by our policies. Please click on the link below for our GDPR Policy which is located on our School Website.

http://www.burradoncommunityprimaryschool.co.uk/data-protection-gdpr/

E-Safety Contacts and References (Appendix 4)

Becta: *www.becta.org.uk/safeguarding*

CEOP (Child Exploitation and Online Protection Centre*):* *www.ceop.police.uk*

CFE e-Safety Officer, KCC Children Families & Education
Rebecca Avery email: esafetyofficer@kent.gov.uk Tel: 01622 221469

Childline: *www.childline.org.uk*

Childnet: *www.childnet.com*

Children's Officer for Training & Development, Child Protection
Mike O'Connell email: mike.oconnell@kent.gov.uk Tel: 01622 696677

Children's Safeguards Service: *www.kenttrustweb.org.uk?safeguards*

Click Clever Click Safe Campaign: *http://clickcleverclicksafe.direct.gov.uk*

Cybermentors: *www.cybermentors.org.uk*

Digizen: *www.digizen.org.uk*

EIS - ICT Support for Schools and ICT Security Advice: *www.eiskent.co.uk?ictsecurity*

Internet Watch Foundation: *www.iwf.org.uk*

Kent e-Safety in Schools Guidance: *www.kenttrustweb.org.uk?esafety (Includes a Schools Audit Tool and Notes on the Legal Framework as part of the PDF versions of this document)*

Kent Primary Advisory e-Safety Pages:
www.kenttrustweb.org.uk/kentict/kentict_home.cfm

Kent Public Service Network (KPSN): *www.kpsn.net*

Kent Safeguarding Children Board (KSCB): *www.kscb.org.uk*

Kidsmart: *www.kidsmart.org.uk*

Schools Broadband Team - Help with filtering and network security: *www.eiskent.co.uk*
Tel: 01622 206040

Schools e-Safety Blog: *www.kenttrustweb.org.uk?esafetyblog*

Teach Today: *http://en.teachtoday.eu*

Think U Know website: *www.thinkuknow.co.uk*

Virtual Global Taskforce — Report Abuse: *www.virtualglobaltaskforce.com*