JOYDENS WOOD JUNIOR SCHOOL

E-Safety Policy

Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance from the UK's Council for Child Safety (UKCISS).

The e-Safety Policy and its implementation will be reviewed annually

This policy is supported by the Social Media Policy and the Mobile Phone Policy.

Revised: May 2018
Review date: May 2019

Signed: ___________________

Headteacher

Joydens Wood Junior School believes that the benefits of ICT and Internet use in school far outweigh the dangers; recognising the issues and planning accordingly will help to ensure appropriate, effective and safe pupil use.

Policy Governance

This policy is designed to ensure safe Internet use by all pupils in school, while online and at home as web based resources are not consistently policed. It is an essential aspect of strategic leadership in the school by all stakeholders. The governors, E-safety officer and SLT team ensure the policy is implemented and reviewed annually to keep abreast with new technologies, safety issues and procedures.

The school keeps a record of all staff and pupils who are granted Internet access. Parents, pupils and staff are asked to sign an acceptable use policy and social media policy when they join Joydens Wood and are provided with details of E-safety through the school website and policy. All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff, prior to using any school computing resource or mobile device. This agreement is held with the AUPs which the school office has.

The E-safety officer is the Headteacher who is also the designated child protection officer and safeguarding person for the school. In their absence, the Deputy and ICT co-ordinator are the next designated people to investigate such matters.

An E-safety incident log is kept by the Headteacher.

Teaching and learning

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

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.
Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

The benefits of using the Internet in education include access to world-wide educational resources, including museums and art galleries.

- Access to learning wherever and whenever convenient.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Exchange of curriculum and administration data with KCC and DfE.
- Educational and cultural exchanges between pupils world-wide.
- Improves access to technical support including remote management of networks and automatic system updates.

How does Internet use enhance learning?

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

How will pupils be taught to evaluate Internet content?

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Kent.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must report immediately to their teacher if they receive any offensive e-mail.
- Staff must report immediately to ICT co-ordinator and SLT if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- 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.
- The forwarding of chain letters is not permitted.
- Whole class or group e-mail addresses will be used.

Published content and the school website

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

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and where possible, will not enable individual pupils to be identified by name.

- Pupils' names will not be used anywhere on the website, particularly in association with photographs which are published on the school website and, occasionally, KLZ (which is password protected and for staff access only).
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or the school's Twitter account.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites for pupils. Key members of staff may access particular social networking sites with permission from the Headteacher.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents are advised that the use of some social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Co-ordinator (via the computing leader).

Managing videoconferencing

- Internet protocol (IP) videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.
- Unique logon and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Managing emerging technologies

Access to the internet is becoming increasingly universal and the internet can now be reached from a wide range of mobiledevices as well as game consoles. The internet technologies pupils and adults are using both inside and outside the classroom can include:

~ Websites
~ Learning platforms including apps
~ Email
~ Instant messaging especially through game consoles and internet
applications on mobile devices
~ Blogs, Vlogs and Wikis
~ Video broadcasting such as You Tube
~ Music downloading
~ Gaming
~ Smart devices with access to the Internet including television and watches
~ Mobile and tablet devices such as Learn Pads with web functionality

~ Social interaction through networking websites
~ Photo applications

This policy takes into account the above devices and other alternatives to ensure the safety of pupils on the internet.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Only year 6 pupils are allowed to bring mobile phones to school. Pupils' phones must be handed into the school office at the beginning of the day for safe keeping.
- Staff will use a school phone where contact with pupils is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school will comply to the GDPR from 25th May 2018.

School E-safety development

The school is developing use of the 360 degree safe self-review audit tool document http://www.360safe.org.uk/Home to review and implement current practice. 'It provides information and stimulus that can influence the production or review of e-safety policies and develop good practice. The tool also provides an evaluative process for identifying strengths and areas for development, while also giving a continuum for schools to discuss how they might move from a basic level provision for E-safety to practice that is aspirational and innovative.'.

E-safety has increasing regard in the computing action development plan and specific actions to develop this area further are outlined and discussed with the SLT team, governors and staff. This is also detailed in the computing Self Evaluation process.

Governor and staff professional development
Governors have access to the KCC governor training sessions on safeguarding which includes E-safety. Governors acknowledge whether they have attended this specific training at Governor meetings which is then recorded in the minutes.

All staff have annual E-safety training which covers new technologies, internet safety issues, current statistics, staff confidentiality, dangers of social networking accounts and looks at the school procedures as well as reviewing the school policy. A register of the staff who attend these sessions is recorded. All AUP forms are updated annually and signed by all staff.

Parent E-safety development

The school encourages e-safety parent workshops each year which is led by the computing co-ordinator and, where appropriate, a member of staff from the local authority. Parents have access to additional information on the school website and links to a variety of websites.

The school will distribute magazines to parents on e-safety and update parents with letters or via newsletter if it is felt parents need to know about certain aspects of e-safety.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents will be asked to sign and return the school's Home-School Internet Agreement.

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 KCC 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.

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 Headteacher, via the computing co-ordinator.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents are informed of the complaints procedure in our Complaints Policy.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet

- 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 for example, social networking sites and will offer appropriate advice.

Communications Policy:

Governor responsibilities

The governors monitor E-safety through Governing body meetings and through visits to the school whilst checking the school's systems for educating the pupils E-safety education. Governors ensure a suitable policy, systems and AUP forms are in place to keep pupils safe through working alongside the school Headteacher. Staff and Governor acceptable use forms are reviewed and renewed annually. This is monitored by a Safeguarding governor and the Chair of governors regularly.

Staff responsibilities

- Staff should ensure the following is adhered to while being employed at Joydens Wood Junior School. Some of this also applies to the Governing body as indicated.
- Staff should always check any website prior to using it for their teacher input or for pupils to use in class so inappropriate content does not appear within a lesson.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses. Contact should be made through the school office official email address. (including.governors) or the staff's own school email address.
- Emails sent to external organisations should be written carefully and professionally with appropriate Standard English before sending, in the same way as a letter written on school headed paper.
- Staff are advised to employ caution when posting any material on the Internet (including social networking sites such as Facebook) relating to themselves and their activities. The golden rule is to ensure that there would be no embarrassment or other consequences if something were read by the Headteacher, governors, parents or pupils of Joydens Wood (inc. governors).
- Staff are advised that, once posted on the Internet, personal material may be publically available for many years as a global footprint is captured. Remembering that sometimes your image/s may be 'tagged' by other friends and acquaintances.
- Staff are advised to use social networking sites with caution (including You Tube, Twitter, Facebook) and to use the security features to ensure maximum privacy settings.
- Under no circumstances are staff allowed to accept a student or ex-students as a 'friend' on any site unless they are a close direct relative such as a (son/daughter/brother/sister). (inc. governors)
- Under no circumstances should staff have images or videos of pupils on their personal mobile devices, cameras or other devices and not be used on school visits or trips. (inc. governors)
- Staff bringing personal devices into school such as mobile phones, ipads should ensure there is no inappropriate or illegal content on the device. (inc. governors)
- Staff who have school owned devices, such as laptops should always present their device to the school's ICT technician for regular updates or monitoring. School resources should not be used at home to look at any inappropriate material or social networking.
- Staff are responsible for keeping their network and email logins secure and to lock their work stations when they are away from their desk or room to avoid child access.
- If staff or pupils discover an unsuitable site in school, the screen must be switched off/closed and the incident reported immediately to the E-safety officer if appropriate.
- Staff should only use the school computing resources for educational purposes which comply with their job description.
- Staff must report E-safety disclosures to the E-safety officer (or in their absence the Deputy or ICT co-ordinator) straight away and log this in the same manner as the school's Safeguarding procedures.
- If staff have concerns over another member of staff and their activity online, this should also be reported straight to the Headteacher.

Parent partnership responsibilities

- Joydens Wood Junior School believes it is essential for parents and the school to work together collaboratively to ensure all stakeholders are fully involved in promoting E-safety both in and out of school.
- Parents' attention will be drawn to the school's E-Safety policy in newsletters, the school prospectus and on the website.
- The school asks that parents refrain from their child bringing in mobile devices into school unless it is absolutely necessary and should this be the case, the device should be left in the front office at the start of the day and picked up after school finishes.
- Parents should not allow their child/children to have mobile devices or other electronic devices on school trips, especially residential trips.
- Parents are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain when joining Joydens Wood.
- Parents are asked to read through and sign the Acceptable Use Agreement with their children at home and talk with them on how to stay safe online.
- Regular information is provided to parents via the school website, newsletters, E-safety workshops and at consultation evenings in relation to E-safety and we ask that parents read this carefully and should they need to discuss any of the information further to contact the E-safety officer or the Head/Deputy.
- Parents are permitted to take photographs and videos at school events for their own personal use only (unless this is expressly prohibited – for example at school plays where there are third party copyright regulations which prohibit recordings).
- Images taken within the school should not be uploaded to social networking sites, especially if a child is in school uniform or another parent's child is present in the image. Recording other than private use would require the written consent of other parents whose child/children may be captured on film or image. Without this consent, the Data Protection Act 1988 and GDPR would be breached.
- Parents are asked to remind their child/children about the dangers of social networking sites and instant messaging on mobile devices and game consoles especially as they become more independent further up into key stage two.
- Parents should be assured that Internet issues will be handled sensitively to inform parents without undue alarm. A partnership approach is encouraged and open door policy with staff is present at the school.

Pupil responsibilities to staying safe online and introducing the E-safety policy across the school

At Joydens Wood, we understand the responsibility to educate pupils in E-safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom. The school ensures the following guidelines, education and warnings are given to pupils during their time at school.

~ All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

~ Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once on line as a global footprint is left.

~ Pupils are always reminded to NOT give out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, email address, specific hobbies or interests).

~ Pupils are encouraged to be wary about publishing specific and detailed private thoughts online (including instant messaging and through interaction with others on game console devices).

~ Pupils are encouraged not to have a Facebook or other social networking accounts as the majority of these sites have an age restriction of 13 or even 16.

~ The staff will regularly monitor a range of popular interactive internet sites to ensure that no inappropriate material has been posted.

~ Pupils are aware that the school network and Internet use is monitored through regular reminders with their teachers and during assemblies.

~ An E-safety assembly will be presented to pupils at the start of each year and again during the annual 'Safer Internet Day' as well as reminders by class teachers.

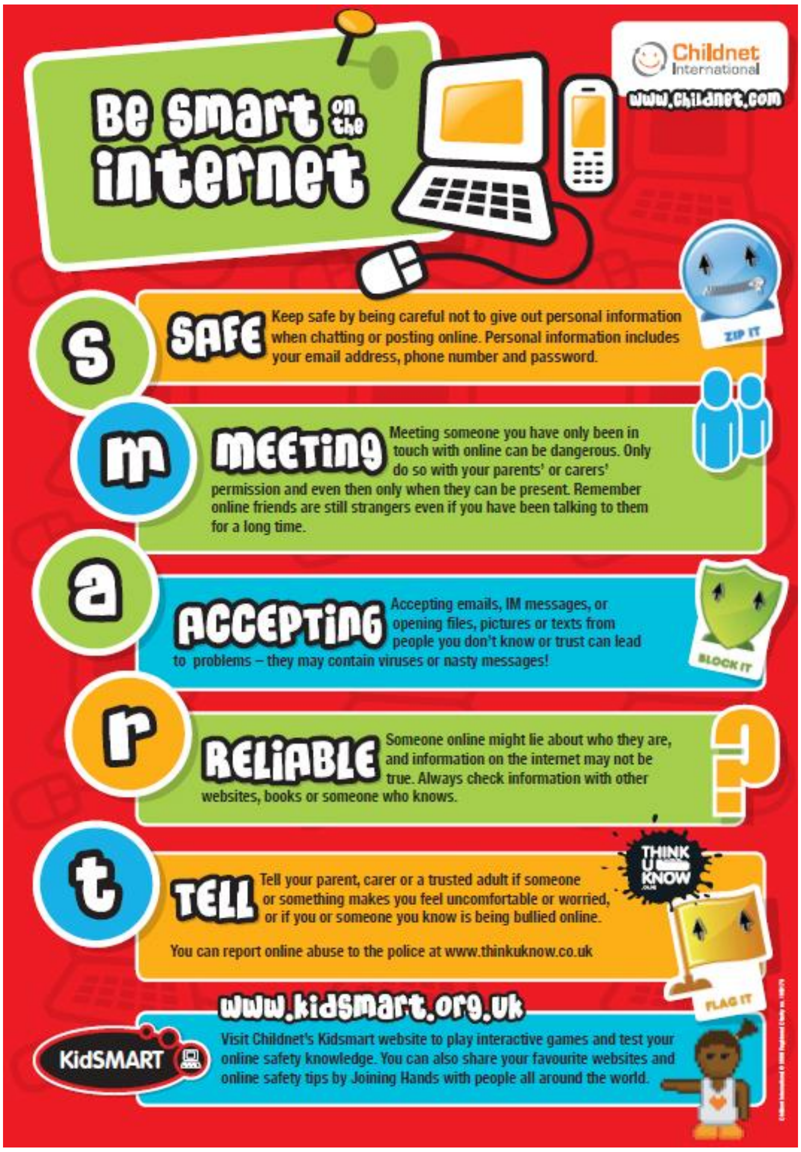
~ The E-safety SMART rules will be displayed in all classrooms. Class teachers remind pupils to report inappropriate material or 'pop ups' should this appear when online. SMART posters will also be displayed by each computer terminal in the classes.

~ The school asks pupils to report any incidents of cyber-bullying to the school via their class teacher or another adult which they feel comfortable in sharing this information.

Special Educational Needs, Inclusion and Equal Opportunities

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid future development of new technologies being used in school and educating pupils about the school's E-safety rules and guidelines. However, the school recognises that pupils with additional needs, may need to have different reminders, prompts or taught using a different approach to meet the needs of an individual whilst enabling them to have the same positive outcome as their peers.

Displayed by each computer in the classroom:



Be Smart on the internet

Childnet International

www.childnet.com

S SAFE Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

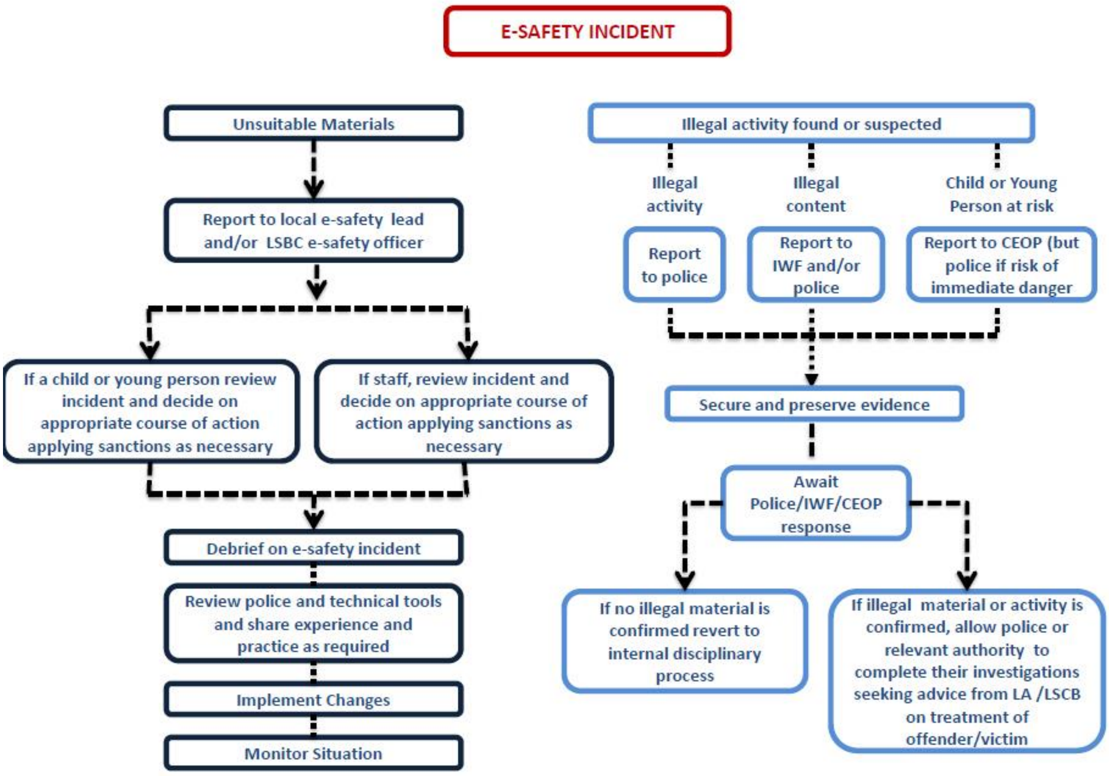
E-safety reporting procedures

Complaints and reports relating to E-safety should be made initially to the E-safety officer who will then liaise with other members of staff/pupils/parents as appropriate. The only exception to this is with incidents of Cyber-bullying when a class teacher is generally the first point of contact. The teacher should make a log of the incident and speak to the E-safety officer (or Head/Deputy in their absence).

Reports of a child protection nature must be dealt with in accordance with school Safeguarding procedures.

If the complaint or incident is about a member of staff or governor, this should go to the Headteacher straight away

BECTA Flowchart for responding to e-safety incidents


E-SAFETY INCIDENT
Unsuitable Materials
Report to local e-safety lead and/or LSBC e-safety officer
If a child or young person review incident and decide on appropriate course of action applying sanctions as necessary
If staff, review incident and decide on appropriate course of action applying sanctions as necessary
Debrief on e-safety incident
Review police and technical tools and share experience and practice as required
Implement Changes
Monitor Situation
Illegal activity found or suspected
Illegal activity
Illegal content
Child or Young Person at risk
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger
Secure and preserve evidence
Await Police/IWF/CEOP response
If no illegal material is confirmed revert to internal disciplinary process
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations seeking advice from LA /LSCB on treatment of offender/victim

Writing and reviewing the e-safety policy

Joydens Wood Junior School is aware of its responsibility when writing policies under current legislation and takes into account; GDPR, Data Protection Act 1998, The Telecommunications (Lawful Business Practice), (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, safeguarding and child protection, social media and mobile phone.

The Headteacher is the e-Safety Coordinator and is also the Designated Child Protection Coordinator as the roles overlap.

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.

The E-Safety Policy was revised by: the computing co-ordinator, Deputy Headteacher and Headteacher.

May 2018

Appendix 1: Internet use - Possible teaching and learning activities

Activities	**Key e-safety issues**	**Relevant websites**
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK Kent Grid for Learning (Tunbridge Wells Network)
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Ask Jeeves for kids - Yahooligans - CBBC Search - Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM EasyMail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Kent Grid for Learning Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Skype FlashMeeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum