JOHN E.BATTY PRIMARY SCHOOL

E-Safety Policy

John Emmerson Batty Primary School

E-Safety
Policy

Supporting our
21st Century vision for
safe learning

JOHN E.BATTY PRIMARY SCHOOL
E-Safety Policy

Responsibility for writing

Our school internet policy has been created by the Head Teacher and Computing Leader using information from BECTa, Redcar and Cleveland Local Authority and government guidance. It has been discussed by the whole staff and approved by governors, who realise how intrinsic to the running of the school, both at a management level and an educational level, the internet is. This policy seeks to ensure users know what good practice is and outlines steps and procedures that will be taken when the darker side of the internet shows itself. It will be reviewed annually.

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks

Teaching and Learning

JOHN E.BATTY PRIMARY SCHOOL
E-Safety Policy

Why is Internet use important?

- 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 use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.
- 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?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries; inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- 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 support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Redcar and Cleveland Council and DCSF;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Pupils in all classes in school will have access to the internet. Access will be designed expressly for pupil and staff use and will include filtering appropriate to the age of the child and responsibilities of the member of staff. However the different types of Internet use are outlined below:

- Online content (e.g., CBeebies) will often be used by the teachers for specific tasks. In these situations the pupils are not searching the internet or navigating away from the page/s and tasks that have been set. Teachers **will have previewed** the site to ensure that it matches the learning outcomes of the lesson/setting. With younger pupils it is essential that access to navigate away accidentally is denied (i.e. hiding the address bar)

- Searchable cached sites will allow access within a site but not beyond it.

- Pupils from Year 3 onwards will use a safe search engine such as Yahooligans, Safari, (Dolphin, Puffin Academy – i-Pads) or Google (safe search through the local authority provision) when searching for information. This is not a failsafe way of preventing access to inappropriate sites but is a good line of defence. Searches will only be permitted when a member of staff is present. Where possible teachers should have pre-searched for the topic in hand and previewed the hits that will be used based on the fact that search engines do not necessarily give the most appropriate site at the top of their lists

- **In most cases, to avoid fruitless hours of browsing, a key website/s will be identified by the teacher for the pupils to use to find information**

(Appendix 1 – Lists possible teaching and learning activities.)

How will pupils learn to evaluate Internet content?

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- The following statements require adaptation according to the pupils' age:
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

Managing Information Systems

How will information systems security be maintained?

- Users must take responsibility for their network use.
- Servers are located securely and physical access restricted.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with LA
- Access by wireless devices is pro-actively managed.
- All Internet connections are arranged via the school's 10Mb broadband connection which is provided by the Local Authority. This in turn links into the Northern Grid network and ultimately the National Education Network. The filters at each stage are extensive and include lists of illegal sites/inappropriate sites that cannot be accessed. It also allows open access and sharing of resources between educational establishments.
- However, when dealing with the internet there is never a failsafe way of blocking inappropriate content in all situations and therefore the school cannot take responsibility for these events when all reasonable steps outlined below have been taken.
- Files held on the school's network will be regularly checked.
- The Computing leader/School Computing technician/LA ICT technician will review system capacity regularly.
- Pupils will inevitably access the internet outside of school. We therefore aim to educate them about internet safety, not simply cover their eyes.

How will e-mail be managed?

Pupils

Pupils from Year 4, 5 and 6 will be given a "professional" email account. The account is set up using Office 365. The pupils are at liberty to use their accounts for correspondence between anyone registered on the jebatty.rac.sch.uk domain. They must ask a member of staff before using it to contact or reply to anyone else not registered as a user on the J.E. Batty Learning Platform. Passwords will be issued by the subject leader. Users agree through the home/school Computing and E-Safety agreement form to keep passwords secret from anyone else apart from the Computing subject leader and their parents.

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- The forwarding of chain letters is not permitted.

The email system has a powerful filter which will automatically direct emails with inappropriate language to the administrator account. This account will be checked through the forwarding of inappropriate mail to the Head Teacher's professional email account.

- Use of personal email accounts by pupils in school is not permitted.
- Use of newsgroups, forums, chat-rooms or social networking sites, by pupils in school, is not permitted unless located on the learning platform.

All of the above information is found in the home/school agreement which must be signed by both the parent/guardian and the child **before a** user account is allocated. Failure to adhere to the agreement will result in suspension of access rights to the internet and email accounts for the individual child until the agreement is signed up to.

Staff

Staff will be given a "professional" email account. The account is also set up using Office 365. The staff are at liberty to use their accounts for correspondence between one another or other professional bodies as part of their work. Passwords must be changed. Users agree through the staff computing and E-Safety agreement form, to keep passwords secret, even from their family and friends.

The email system has a powerful filter which will automatically direct emails with inappropriate language to the administrator account. This account will be checked through the forwarding of inappropriate mail to the Head Teacher's professional email account. In this way possible abuse of the system will be monitored.

- Users will also be expected to report any offensive emails that they receive to a Senior Team Leader.
- Any intercepted emails or reports of offensive emails will be reported to the Head Teacher.
- The Head Teacher and system Administrator will have the right to have access to all staff member's professional email accounts and learning platform pages.
- Use of personal email accounts in school is permitted only in circumstances where this is done in the staff's own time (e.g. lunch time) and where no pupils are present.
- Use of personal email accounts in dedicated teaching time is not permitted in any circumstance.
- Use of newsgroups, forums, chat-rooms or social networking sites in school is not permitted unless located during staff's own time (e.g. lunch time, after school) and when no pupils are present.

The staff internet agreement form sets out the terms and conditions that they must agree to **before** being allocated an account. Failure to adhere to the agreement will result in suspension of internet access rights for the individual and may result in disciplinary measure being taken by the governing body.

School's Intranet

Use of Shared Site Pages

Pupils will become part of school shared sites on the learning platform **ONLY WHEN** a group is set up e.g. Lego team page

- All pupils, through discussion and the home/school agreement will be taught to understand that these shared sites are professional sites and that their use for inappropriate behaviour will be noted. Such behaviour will result in suspension of access rights and appropriate consequences in line with the behaviour and discipline policy.
- These shared sites have a specific list of people who can access them. Parents and staff will have the right to contact the Head Teacher and to discuss who else is invited to be a member of a site if they feel that there is an issue with who is accessing information relating to their child.
- The Freedom of Information Act will be referred and adhered to in terms of what information can freely be accessed or requested.

There may be photographs of pupils on shared sites to celebrate achievement or share ideas within school or even across schools.

- Pupils will not be identified by name in such cases and will not be allowed to post their own pictures unless first checked by an adult.
- Access is restricted and can be discussed with the Head Teacher.

Staff will become part of staff sites on the learning platform **ONLY WHEN** the school agreement has been signed e.g. Staff site

- All pupils, through discussion and the home/school agreement will be taught to understand that these sites are professional sites and that their use for inappropriate behaviour will be noted. Such behaviour

will result in suspension of access rights and appropriate consequences in line with the behaviour and discipline policy.
- These sites have a specific list of people who can access them. Parents and staff will have the right to contact the Head Teacher and to discuss who else is invited to be a member of a site if they feel that there is an issue with who is accessing information relating to their child.
- The Freedom of Information Act will be referred and adhered to in terms of what information can freely be accessed or requested.

There may be photographs of pupils on shared sites to celebrate achievement or share ideas within school or even across schools.
- Pupils will not be identified by name in such cases and will not be allowed to post their own pictures unless first checked by an adult.
- Access is restricted and can be discussed with the Head Teacher.

Emerging and Wireless Technologies

Management

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out using the LA checklist **(See Appendix 2)** before purchase and use in school is allowed.
- Mobile phones will not be allowed in school, to be used during lessons or formal school time by pupils, but may be used by staff during staff non-teaching/personal time (E.g. breaks and lunchtime) and when only when pupils are **NOT** present.

Wireless Network security

- The school's wireless network is encrypted by the school ICT technician through Redcar and Cleveland LA provided by the ICT Service Level Agreement, so as to prevent unauthorised access.
- It has been checked and authorised by the LA network administration team.
- If a breach in security is discovered it will be reported to the Head Teacher and steps will be taken to review the security level in place with relevant specialists.
- Accidental access to inappropriate material will be reported on the Computing accidental access chart kept in the Computing suite. This will be monitored on a daily basis by the school computing support technician
- Staff are permitted to access their personal wireless connection to the internet at their place of residence, but no user should attempt to use the school's computing equipment to access any network other than the school's network or personal home network.

Use of mobile devices

- Pupils are not permitted to have mobile phones in school. Failure to observe this will result in confiscation.
- Use of mobile phones by parents and other visitors when in school is permitted only when they are outside of the building.
- Use of mobile phones by staff in school is permitted only in circumstances where this is done during non-teaching/non-contact/personal time and when pupils are **NOT** present.
- Use of mobile phones during dedicated teaching time, or during staff meetings is not permitted in any circumstance. Mobile phones should be switched off or set to silent during these times.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters, the school brochure and on the school website.
- School seek the views of parents on the policy on a regular basis using annual parent/carer surveys and through the provision of information within the newsletter.

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Any parent / carer concerned about the use or teaching of computing in school should contact the Computing Leader in the first instance. The Computing leader will then liaise as appropriate with other staff members and the Head Teacher in an attempt to engage with these concerns.
- Where a parent/carer has a complaint about any use of computing within school the school's complaints policy should be adhered to.
- The views of any parents/carers with specific religious beliefs on the use of technology will be considered.

Admin Network

The school adheres to the LA policy regarding use of the administration machines.

Internet Policy Decisions

How will Internet access be authorised?

Pupils will not be allowed to access and search the internet unless authorised by a member of staff.

- 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 Information Systems Code of Conduct' before using any school computing resource.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with a password.
- Responsibility for the monitoring of what the pupils find is then the responsibility of that adult.
- Information on when use of searching on the internet is appropriate can be found in the school Scheme of Work for Computing; other uses are the sole responsibility of the supervising adult.
- Appropriate behaviour and understanding of how addresses are composed will be explicitly taught before ever using an internet search in school and will be reinforced by visual reminders.

Accessing and interacting with the internet is part and parcel of many users' reasons for having an internet connection. Therefore internet safety is implicitly taught in Year 1 and Year 2 and repeated throughout Key Stage 2. It will be referred to whenever a unit of work requires use of the internet. Key themes to be covered are listed below:

- Safe browsing on the internet
- Use of mobile technology e.g. phones, tablets etc.
- Use of chatrooms
- Use of blogs, webspace and social networking sites
- Online gaming
- Use of email
- Copyright
- What to do when you come across something that is inappropriate

- Use of the network for personal monetary profit or gambling is strictly forbidden.
- In accordance with the Data Protection Act 1984/98, users are not allowed to access other user's personal files and folders. The exception to this being system administrators who can gain access through permission from the Head Teacher when just cause has been established.
- Staff are made aware of LA Guidelines for data protection through LA documentation sent to all LA employees. (Copy kept in E-Safety box held in computing suite)

- A copy of the LA Safeguarding document is also made available to staff for reference and a copy is kept on the school's learning platform for agreed users to access. (Copy in E-Safety box in computing suite.)

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. Neither the school nor RCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school should audit computing 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.

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.

Communication of Policies

Useful e-safety programmes include:

- Think U Know; currently available for primary pupils and parents. (www.thinkuknow.co.uk/)
- Grid Club www.gridclub.com
- The BBC's ChatGuide: www.bbc.co.uk/chatguide/
- E-Safety rules will be posted in rooms with Internet access.
- Pupils 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.
- Instruction in responsible and safe use should precede Internet access.

How will the policy be discussed with staff?

- All staff will be given the School E-Safety Policy and its application and 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 computing use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-safety policy will be provided as required.

Review of Policies

The effectiveness and usefulness of the Acceptable and Safe use of the Internet will be evaluated by all members of staff should the need arise but no later then 2018.

Policy agreed by the governing body on 2nd March 2016

Signed on behalf of the governing body:
Reviewed: February 2016 By: J Norris

Appendix 1 – 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 The school / cluster VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. 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 Google Safe Search
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail
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. Pupils" work should only be published on „moderated sites" and by the school administrator.	Making the News SuperClubs Plus Headline History National Education Network Gallery
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. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art National Education Network Gallery
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 Plus FlashMeeting
Audio and video conferencing to gather information and share pupils" work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives “On-Line” Global Leap

Appendix 2 – LA checklist for purchasing of technologies