Inmans Primary School

E-Safety Policy

Inmans Primary School e-Safety Policy 2017

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, Anti -Bullying and for Child Protection.

- 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 the Head Teacher and approved by governors.

The e-Safety Policy and its implementation was reviewed by the ICT Co-Ordinator in January 2014 and will be reviewed annually or as and when necessary updates need to be made.

Teaching and learning

Why Internet use is important

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

Internet use benefits education

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- 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;
- exchange of curriculum and administration data with LEA and DfE;

- access to learning wherever and whenever convenient.

Internet use will enhance learning

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

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Pupils will be taught how 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.
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Managing Internet Access and Information Systems

Information system security

- Where possible, all information storage shall be restricted to only necessary users. Access granted to new groups of users shall be approved by the person in charge of data security (ICT Technician).
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- The use of user logins and passwords to access the school network will be enforced.
- Unapproved software will not be allowed in pupils'/staff work areas or attached to e mails.
- The person in charge of network management will review system capacity regularly.
- Security strategies will be discussed with the LEA.

E-mail

- Pupils may only use approved e-mail accounts on the school system for school purposes.
- Pupils must immediately tell a teacher if they receive an 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.

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 pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' 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 images/videos of pupils are electronically published.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Managing filtering

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

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.

- The school will work with the LEA, DfES 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 Coordinator.
- Any material that the school believes is illegal will be reported to appropriate agencies such as Humberside Police or CEOP.

Managing videoconferencing

- 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.
- 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.

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. The sending of abusive or inappropriate text messages is forbidden.
- 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.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT User Agreement' before using any school ICT resource.
- Parents and pupils will be asked to read and sign the "Rules for responsible Internet use" and return to school.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the Internet is granted under supervision paying particular attention to the "Rules for Responsible Internet Use".

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Humberside Police.

Responding to incidents of concern

- All reported incidents and actions will be recorded in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.

- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the Head Teacher under the Complaints procedure.
- Any complaint about staff misuse must be referred to the Head Teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

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, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

How will Cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated at Inmans Primary School. Full details are set out in the schools policy on anti-bullying and behaviour.
- All incidents of cyberbullying reported to school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

Mobile phones and personal devices

Pupils Use of Personal Devices

- Mobile phones are not permitted during the school day. Parent/carers must notify the Head Teacher if they request their child to bring a mobile phone to school. These will be handed in at the beginning of the school day and then handed back at the end of the school day.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released at the end of the school day.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will use the school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode and will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in networked rooms and discussed with the pupils at the start of each year.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Pupils will be informed that network and Internet use will be monitored.

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.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Enlisting parents' support

- Parents and pupils will be asked to read and sign the school Acceptable User Policy and discuss its implications.

- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use.

To be reviewed May 2017