Pattishall Primary is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.

E- Safety Policy

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Pattishall we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.
"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."
From: Safeguarding Children in a Digital World. BECTA 2006

Our e-safety policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors. The e-safety policy and its implementation shall be reviewed annually.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the Governors will include the monitoring of e-safety incident logs.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety is delegated to the teachers.
- The Headteacher/Senior Leaders are responsible for ensuring that the staff receive suitable CPD to enable them to carry out their e-safety roles.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

Staff:

- Take day-to day-responsibility for e-safety issues.
- Liaise with school ICT coordinator.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with ISP to ensure filtering systems are as effective as possible.

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Pupils may only use approved e-mail accounts on the school system.
- 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.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.

- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Social Networking

- Social networking Internet sites (such as Facebook and Instagram) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites in school is not allowed.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting

All breaches of the e-safety policy need to be reported to the Headteacher. The details of the user, date and incident should be provided.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Safeguarding Lead immediately – it is their responsibility to decide on appropriate action not the class teachers.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline)

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying or inappropriate contact.

- Pupils, by permission of the Headteacher, can bring mobile phones onto the school site where it is seen by the school as precautionary use. These are handed in to the child's teacher at 8:45am and collected at the end of the day.

- The sending of abusive or inappropriate text messages is forbidden.
- Parents cannot use mobile phones on school trips to take pictures of the children.
- On trips staff mobiles are used for emergency only

Digital/Video Cameras/Photographs

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- Parent(s)/guardian(s), and others present at school events, will be informed that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.
- Staff using personal cameras to capture images should ensure that the photographs are transferred to the school's server before leaving the premises. Photos taken by the school are subject to the Data Protection act.

Published Content and the School Website

The school website is a valuable source of information for current and potential parents.

- Contact details on the website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

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

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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.
- Complaints of a child protection nature shall be dealt with in accordance with the school's child protection procedures.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

- Pupils will be informed that Internet use will be monitored.

Staff:

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

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

Further Resources

We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".

This policy is linked directly to the following:

- Behaviour Policy
- Child Protection & Safeguarding Policy
- Curriculum policies