PENDRAGON PRIMARY SCHOOL

ESAFETY POLICY

LEAD PERSON: Computing/ Esafety Subject Leader

AGREED BY STAFF: June 2015

AGREED BY GOVERNORS: Autumn 2015

REVIEW DATE: June 2016

Esafety Policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school:

- **the ground rules we have developed in school for using the Internet and online technologies**
- **how these fit into the wider context of our other school policies**
- **the methods used to protect children from sites containing pornography, racist or politically extreme views and violence**.

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the school shares with parents and carers. At Pendragon Primary School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

The development of our safety policy involved…

- **Miss C Shaw - Headteacher**
- **Mr C Jones – E Safety Coordinator**

It will be available on school website, the school server and by request to the school office.

Rationale

At Pendragon Primary School we believe that the use of information and communication technologies in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement. Yet at the same time we recognise that 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.*

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction.

Benefits of using online technologies in education include:

- Access to world-wide educational resources
- Inclusion in the National Education Network (NEN) connecting all UK schools and resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration across schools, networks of schools and services

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. At Pendragon Primary School we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials (see appendices).

We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using the internet. Members of staff constantly monitor pupils' use of the internet and other technologies and are able to monitor pupils' use of Starz communication and publishing tools. Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities.

Messages involving Risks and Rules and Responsibilities are taught and/or reinforced as detailed in the school's Acceptable Use Policies (see appendices).

Technology In School

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service.

E2BN's Protex web filtering system received full Becta (British Educational Communications and Technology Agency) accreditation in 2007 by blocking over 90% of all inappropriate material. E2BN also manage a distributed caching service which is integrated with the web filtering service.

Ref: E2BN Website

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUPs and e-safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Technologies regularly used by pupils and adult stakeholders include:

Staff:

- Laptops and desktops
- Cameras and video cameras, visualisers
- Internet, E-mail, Starz Learning Platform, central hosting including access to SIMS and confidential pupil information

Pupils:

- Laptops and desktops
- iPads
- Cameras and video cameras, visualisers
- Internet, Starz Learning Platform including e-mail, discussion forums, blogs and other communication tools
- Other peripherals such as programmable toys, dataloggers, control technology equipment

Governors:

- *Laptops and desktops*
- *Mobile phones and tablets*
- *Cameras and video cameras, visualisers*
- *Internet, E-mail, Starz Learning Platform*

IT Technicians

- *Full access to all of the above for maintenance, updating and service..*

Others on school premises:

- *Limited access to school systems such as filtered internet access.*

Whilst we recognise the benefits of individual pupil logins to our school network, in KS1 we prefer to use year group logins for ease of access. As pupil move into KS2 they will then start to use individual logins. All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password. The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office. School staff and pupils are **not** permitted to connect personal devices to the school's wireless network and the wireless key is **not** given to visitors to the school.

The ESafety Curriculum

In line with recommendations in the ESafety briefing for Ofsted Inspectors (Sept 2012) we have planned a range of age-related teaching and learning opportunities to help our pupils to become safe and responsible users of new technologies. These opportunities include:

- Termly Key stage assemblies
- Specific activities during safety week, held in February and Anti-bullying week, held in November
- Age-relate classroom activities using the ThinkUKnow materials
- ACE accredited scheme for pupils
- Related work in PSHE lessons
- Posters and reminders in and around the school
- Specific teaching and notification for school staff in an incident occurs

Safeguarding Children Online

Our School recognises that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We acknowledge the need to:

Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.

UKCCIS (The UK Council for Child Internet Safety) – June 2008

The school has published Acceptable Use Policies for pupils and staff who sign to indicate their acceptance of our AUPs and relevant sanctions which will be applied should rules be broken. Please see appendices for full details.

Any known or suspicious online misuse or problem will be reported to the designated E-Safety Co-ordinator for investigation/ action/ sanctions.

Responding to Incidents – *(Education Child Protection Service – June 2010)*

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology. It is important that responses to e-safety incidents are consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.

If an e-safety incident occurs, Pendragon Primary School will follow its agreed procedures for dealing with incidents including internal sanctions and involvement of parents (for Computing, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix). Where the school suspects that an incident may be a Child Protection issue, the usual Child Protection procedures will be followed.

Dealing with Incidents and Seeking Help

If a concern is raised, refer immediately to one of the designated persons for child protection. If that is not possible refer to the headteacher, another member of the Senior Leadership Team or, if necessary, the Chair of Governors(SEN governor).

It is their responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator

Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the Education Child Protection Service helpline.

Step 3: Ensure that the incident is documented using the standard child protection incident logging form (see appendix)

Depending on the judgements made at steps 1 and 2 the following actions should be taken:

Staff accused – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.

Staff victim – Seek advice from your Human Resources (HR) provider and/or Educational Child Protection Service

Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue

Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline.

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the agreed procedures for dealing with any allegation against a member of staff (see appendix).

Terms used in this policy

AUP: Acceptable Use Policy.

A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse.

Child: Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday.

E-safety: We use e-safety, and related terms such as 'online', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose e-safety risks. We try to avoid using the term 'ICT' when talking about e-safety as this implies that it is a technical issue – which is not the case. The primary focus of e-safety is child protection: the issues should never be passed solely to technical staff to address.

PIES: A model for limiting e-safety risks based on a combined approach to **P**olicies, **I**nfrastructure and **E**ducation, underpinned by **S**tandards and inspection. Whilst not explicitly mentioned in this policy, this model provides the basis for the school's approach to e-safety.

Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-safety is just one aspect of a much wider safeguarding agenda within the UK, under the banner of *Every Child Matters: Change for Children*. Those with responsibility for the development and delivery of e-safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children and young people in their care.

Schools: For ease of reading we refer predominantly to schools within this publication, but the underlying principles can be applied equally to any setting with responsibility for educating or safeguarding children and young people.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an AUP. This might be pupils, staff, parents and carers, or members of the wider community, depending on provisions of your AUP or the context in which you operate.

Appendices/Cross references:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)
- Behaviour policy
- Safeguarding and Child Protection
- SRE (Sex and Relationships Education)
- Safer Working Practices
- Data Protection Policy
- County guidance (e.g. Use of Digital Images, e-mail)
- AUPs- staff, pupil,(KS2), (KS1)
- Anti-Bullying Policy
- School Complaints Procedure
- LA Infrastructure guidance (E2BN)
- Cambridgeshire Progression in ICT Capability Materials
- Risk assessment log
- Incident Log
- Computing Policy

Communication Technologies in school	Staff and other adults				Pupils				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with SLT permission	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	*						*		
Use of mobile phones in lessons		*					*		
Use of mobile phones in social time	*								*
Taking photos on personal mobile phones or other camera devices				*					*
Use of hand held devices eg PDAs, PSPs		*							*
Use of personal email addresses in school, or on school network		*							*
Use of school email for personal emails				*					
Use of chat rooms / facilities (excluding school approved)				*					*
Use of instant messaging (excluding school approved)				*					*
Use of social networking sites (excluding school approved)				*					*
Use of blogs (through Starz)	*				*				
Use of Skype, IM and video conferencing		*							*

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					*
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					*
	adult material that potentially breaches the Obscene Publications Act in the UK					*
	criminally racist material in UK					*
	pornography				*	
	promotion of any kind of discrimination				*	
	promotion of racial or religious hatred				*	
	threatening behaviour, including promotion of physical violence or mental harm				*	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.				*	
Using school systems to run a private business					*	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					*	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					*	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						*
Creating or propagating computer viruses or other harmful files					*	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					*	
On-line gaming (educational)			*			
On-line gaming (non educational)					*	
On-line gambling					*	
On-line shopping / commerce			*			
File sharing			*			
Use of social networking sites					*	
Use of video broadcasting eg Youtube			*			

Incidents: All incidents to be reported to SLT and E-safety Co-ordinator.	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	
Unauthorised use of non-educational sites during lessons	
Unauthorised use of mobile phone / digital camera / other handheld device	
Unauthorised use of social networking / instant messaging / personal email	
Unauthorised downloading or uploading of files	
Allowing others to access school network by sharing username and passwords	
Attempting to access or accessing the school network, using another student's / pupil's account	
Attempting to access or accessing the school network, using the account of a member of staff	
Corrupting or destroying the data of other users	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	
Continued infringements of the above, following previous warnings or sanctions	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	
Using proxy sites or other means to subvert the school's filtering system	
Accidentally accessing offensive or pornographic material and failing to report the incident	
Deliberately accessing or trying to access offensive or pornographic material	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	