E-Safety Policy

2016-2017

Stow Heath Primary School

Approved Date:

Chair of Governors:

Headteacher:

Review date:

Introduction
At Stow Heath Primary School we believe that our children need to have the opportunity to explore, investigate and to be challenged. We maintain that learning should be a rewarding and enjoyable experience. Through our teaching we aim to equip our children with the skills, knowledge and understanding to make choices. We recognise and support the LA's impetus for raising standards through the quality of teaching and learning.

This policy document needs to be read in conjunction with the Foundation Curriculum, the National Curriculum 2000 for Information and Communication Technology, especially the programme of the Study and Attainment Targets for assessment, the Digital Safeguarding policy and the QCA Information Technology document and Wolverhampton's e-confident learner framework.

Aims
Through our teaching of ICT we aim to enable our children to:
- Provide a broad and balanced curriculum designed to meet the needs of all our children, with equal opportunities and access for all.
- Provide the best possible educational opportunities for all our children to achieve their full potential and to develop confidence and competence when working in ICT to become e-confident learners.
- Offer a curriculum that is enhanced by integrating ICT across all subject areas, promoting enjoyment, a personal sense of fulfilment, achievement and the life skills that will help our children thrive in the 21st century.

Through ICT we can also:
- Develop speaking and listening skills through group work and discussion
- Develop cross curricular links through careful planning and reinforce skills from the core subjects literacy and numeracy through ICT and of foundation subjects Art and design, Geography, History etc.
- Ensure continuity and progression of skills, knowledge and understanding through the school schemes of work. It clearly identifies the learning objectives and expectations for each year group.
- Ensure the children understand the effects and limitations of ICT and makes choices about its suitability for a particular task.
- Develop understanding of the relevance and application of |ICT within school and in everyday life

E-Learning policy Statement:

At Stow Heath Primary School, the term 'e-learning' incorporates all learning and teaching facilitated and supported through the use of digital technology. E-learning creates engaging learning opportunities and, when effectively implemented, acts as a catalyst for authentic, meaningful learning experiences.
The developments within our school reflect government investment and local innovation.

Mission Statement for E-Learning:

To enhance teaching and learning throughout the school we fully integrate digital technology into all aspects of the curriculum, through the use of creative technology and the contribution of well trained, competent and enthused staff. This will enable our children to develop the necessary technological skills needed for lifelong learning in the 21st Century.

1. **Legal Framework**
   1.1 This policy has due regard to the following legislation, including, but not limited to:
      - The Human Rights Act 1998
      - The Data Protection Act 1998

- The Regulation of Investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The computer Misuse Act 1990, amended by the Police and Justice Act

1.2 This policy also has regard to the following stator guidance:

- DfE (2016) 'Keeping Children Safe in Education

2. Use of the Internet

2.1 The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2 Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools to implement, which minimise harmful risks.

2.3 When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online video or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.e. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1 It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of the school, and to deal with incidents of such as a priority.

3.2 Safety in the school, keeping in mind data protection requirements.

3.3 The e-safety officer will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.

3.4 The school will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.5 The e-safety officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

3.6 The e-safety officer will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.

3.7 Cyber bullying incidents will be reported in accordance with the school's Antibullying and Harassment Policy.

3.8 The governing body will hold regular meetings with the e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

3.9 The e-safety officer, is responsible for ensuring the day-to-day e-safety in our school, and managing any issues that may arise.

3.10 The headteacher is responsible for ensuring that the e-safety officer and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

3.11 The e-safety officer will provide all relevant training and advice for members of staff on e-safety.

3.12 The headteacher will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety.

3.13 The governing body will evaluate and review this E-safety Policy on a termly basis, taking into account the latest developments in ICT and the feedback from staff/pupils.

3.14 The headteacher will review and amend this policy with the e-safety officer, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

3.15 Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.16 All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.17 All staff and pupils will ensure they understand and adhere to our Acceptable Use Policy, which they must sign and return to the headteacher.

3.18 Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

3.19 The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

3.20 Parents/Carers are responsible for signing the home school agreement which includes permission for the use of photos, videos and internet use

4. E-safety control measures

4.1. Educating pupils:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.

4.2. Educating staff:

- All staff will undergo e-safety training on a termly basis to ensure they are aware of current e-safety issues and any changes to the provision of esafety, as well as current developments in social media and the internet as a whole.
- All staff will undergo regular audits by the e-safety officer in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.

4.3. Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form as part of our Acceptable Use Policy.
- A record will be kept by the headteacher of all pupils who have been granted internet access.
- Pupils' passwords will be changed on a regular basis, and their activity is continuously monitored.
- Management systems (Impero) will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to particular websites.

- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers, supply teachers etc
- The master users' passwords will be available to the headteacher for regular monitoring of activity.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the e-safety officer or safeguarding lead for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy. This is provided by Impero software.

4.4. Email:

- Staff will be given approved email accounts and are only able to use these accounts.
- Use of personal email to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

4.5. Social networking:

- Use of social networking sites and newsgroups in the school, is not allowed and is blocked/filtered,
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.
- Pupils are regularly educated on the implications of posting personal data online, outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

4.6. Published content on the school website and images:

- The headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the school website will be the phone, email and address of the school. No personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school or any information that may affect its reputability.

4.7. Mobile devices, hand-held computers and laptops:

- The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.

- Mobile devices are only allowed to be used during school hours by members of staff in designated areas.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the e-safety officer when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile phones must not be used to take images or videos of pupils or staff.
- The school will be especially alert to instances of cyber bullying and radicalisation and will treat such instances as a matter of high priority.
- All laptops have been set up with an internal hard drive lock and personal usernames and passwords that are required to be changed regularly.

4.8. Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the e-servives representitive.
- ICTS must ensure that the filtering of websites and downloads is up-to-date and monitored. Any breaches of security will be reported to ICTS via email.

	Staff and other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times and in certain places	Allowed for selected staff	Not allowed	Allowed	Allowed a certain times and in certain places	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	X				X			
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking phones on mobil phones/cameras				X				X
Use of other mobile devices eg. Tablets/gaming devices		X						X
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of social media				X				X

5. Cyber bullying

Responsibilities for the prevention of cyber bullying

5.1. The Head Teacher will be in overall charge of the practices and procedures outlined in this policy and will ensure that their effectiveness is monitored.

5.2. The Head Teacher will ensure that the school maintains details of agencies and resources that may assist in preventing and addressing cyber bullying.

5.3. All members of staff will be trained to identify signs of cyber bullying and will be helped to keep informed about the technologies that children commonly use by self-study and regular updates.

5.4. An eSafety Code of Conduct has been developed; AUP and will be reviewed and communicated to help pupils protect themselves.

5.5. Pupils will be advised on cyber bullying through curricular and pastoral activities.

5.6. Pupils and staff are required to comply with the school's Acceptable Computer Use Policy (AUP).
5.7. The Acceptable Use Policy is discussed at induction.
5.8. Parents/Carers are encouraged to discuss cyber safety and bullying with their child to supplement learning.
5.9. Parents/Carers will be provided with information and advice on cyber bullying.

Required actions if cyber bullying occurs

- Advise the child not to respond to the message.
- Refer to relevant policies including eSafety, acceptable use, anti-bullying and PHSE.
- Secure and preserve any evidence.
- Inform Head teacher and Senior Management team.
- Notify parents of the children involved.
- Consider delivering a parent workshop for the school community.
- Consider informing the sender's e-mail service provider.
- Consider informing the police depending on the severity or repetitious nature of offence.
- Inform the LA eSafety officer.

Required actions if malicious posts or threats are made against students or teachers

- Ensure pupils are shielded from further exposure.
- Inform site and request the comments be removed if the site is administered externally.
- Secure and preserve any evidence including URLs, Screenshots and Printouts.
- Inform Head Teacher and Senior Leadership Team.
- Inform parents.
- Send all the evidence to CEOP.
- Endeavour to trace the origin and inform police as appropriate.
- Inform LA e Safety officer.

Reporting structure

- At Stow Heath Primary School, issues of cyber bullying should be reported along the same chain as our anti-bullying policy.

Responding to cyber bullying

- Cyber bullying will generally be dealt with through the schools anti-bullying policy. A cyber bullying incident might include features different to other forms of bullying, prompting a particular response.
- Key differences might be:
- The impact may be extensive in scale and scope
- The location may be anytime and anywhere nature of cyber bullying
- The anonymous nature of the offence. The person being bullied might not know who their bully is
- The motivation behind the offence. The perpetrator might not realise that his/her actions are bullying
- The evidence of the offence. Unlike traditional bullying, it is not always necessary to rely on witnesses or hearsay, the subject of the bullying may have evidence of what happened

Support for the person being bullied

- The feelings of the victim are paramount and as with any form of bullying, support for the individual will depend on the circumstances. For example:
- Emotional support and reassurance that they haven't done anything wrong
- Reassurance that it was right to report the incident and that something will be done about it
- Liaison with the child's parents/carers to ensure a continuous dialogue of support
- Advice not to retaliate or reply, but to keep the evidence and show or give it to their parent or a member of staff
- Advice on other aspects of the eSafety code of conduct to prevent re-occurrence
- Discussion with the child's parents/carers to evaluate their online habits
- Age appropriate advice on how the perpetrator might be blocked online
- Actions, where possible and appropriate, to have offending material removed
- Discussion with the child's parents/carers on whether police action is required (except in cases of CEOP where the police may be contacted without discussion with parents/carers)

Investigation

- Again, the nature of any investigation will depend on the circumstances and the age of the child.
- Review of evidence and advice to preserve it, for example by saving or printing (e.g. phone messages, texts, emails, website pages)
- Efforts to identify the perpetrator, which may include looking at the media, systems and sites used, however members of staff do not have the authority to search the contents of a phone.
- Identifying and questioning witnesses.
- Contact with the Child Exploitation and Online Protection Centre (CEOP) if images might be illegal or raise child protection issues
- Requesting a pupil to reveal a message or other phone content or confiscating a phone.

Working a perpetrator who is a pupil

- Until such time that the perpetrator is found guilty, they will be considered innocent.
- Work with the perpetrator and any sanctions will be determined on an individual basis, in accordance with the Anti-Bullying Policy, with the intention of:
- Helping the person harmed to feel safe again and be assured that the bullying will stop.
- Holding the perpetrator to account, so they recognise the harm caused and do not repeat the behaviour.
- Helping bullies to recognise the consequences of their actions and facilitating change in their attitude and behaviour.
- Demonstrating that cyber bullying, as any other form of bullying, is unacceptable and that the school has effective ways of dealing with it.

Cyber bullying Education

- As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about eSafety will take place as part of ICT and PSHE.

6. Reporting misuse

6.1. Misuse by pupils:

• Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
• Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher, using a Complaints Form.
• Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
• Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher and will be issued once the pupil is on the school premises.
• Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection Policy.

6.2. Misuse by staff:

• Any misuse of the internet by a member of staff should be immediately reported to the headteacher, using a complaints form.
• The headteacher will deal with such incidents in accordance with the Allegations against Staff Policy, and may decide to take disciplinary action against the member of staff.
• The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Staff Incidents	Refer to headteacher	Refer to LA/HR	Refer to police	Refer to eservices support staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	X	X	X		X	X	X
Inappropriate personal use of the internet/social media/personal email	X				X		X
Unauthorised downloading or uploading of files	X			X			
Allowing others to access school network by sharing userneam and passwords or attempting to access or accessing the school network, using another persons account	X						
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X		
Deliberate actions to breach data protection or network security rules	X				X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X				X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X	
Using personal email/soci\l networking/instant messaging.text messaging to carry out digital communications with students/pupils	X	X	X				X
Actions which could compromise the staff member's professional standing	X	X			X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X	X
Using proxy sites or other means to subvert the schools filtering system	X			X			
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X		

Deliberately accessing or trying to access offensive or pornographic material	X	X	X				X
Continued infringements of the above, following previous warnings or sanctions	X						X

Pupil Incidents	Refer to class teacher	Refer to headteacher	Refer to police	Refer to eservices support staff for action re filtering etc.	Inform parents/carers	Removal od network/internet access rights	warning	Further sanctions eg detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal		X	X		X			
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised/inappropriate use of mobil phone/digital camera/other mobile device		X			X			
Unauthorised/inappropriate use of social media/messaging apps/personal email		X			X			
Allowing others to access school network by sharing username and passwords		X					X	
Attempting to access or accessing the school network, using another pupil's account		X					X	
Attempting to access or accessing the school network, using the account of a member of staff		X					X	
Corrupting or destroying the data of other users		X				X		
Continued infringements of the above, following previous warnings or sanctions		X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X						X
Using proxy sites or other means to subvert the schools filtering system		X				X		X
Accidentally accessing offensive or pornographic material and failing to report the incidentX		X			X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			