The Federation of Shevington Community Primary Schools

E-safety Policy

2016-17

Agreed by Federation Governors

To be reviewed annually.

1 WRITING AND REVIEWING THE E-SAFETY POLICY

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

- Each school has an E-Safety Co-ordinator. This is the Head of School It is not a technical role. These people will be supported by the Child Protection Co-ordinator.
- This E-Safety policy has been written, using the Kent E-Safety Policy as a model alongside local and national Government guidance.
- It will be reviewed annually in light of the fast changing nature of modern technologies.
- All members of the Federation staff have a responsibility to ensure the policy is applied across all areas of school life in all departments.

2 TEACHING AND LEARNING

.Why the Internet and digital communications are important:

- The Internet is an essential element in 21st century life for education, business and social interaction. The School has a duty to provide pupils with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for all staff and pupils.

Internet use will enhance Learning

- The School Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the 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.
- Pupils will be shown how to publish and present information to a wider audience.

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 will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content as part of the Computing Curriculum.

3 MANAGING INTERNET ACCESS

Information System Security

- School ICT systems will be reviewed regularly and this is the responsibility of the ICT co-ordinator in close co-operation with all staff of the school.
- Virus protection will be updated regularly.

- Security strategies will be discussed with the Local Authority as necessary by the ICT Co-ordinator.
- **Forensic monitoring software is installed on all computers and will be accessed by school office staff and members of the Senior Management Team. (SECURUS SOFTWARE)**
- **At the present time ipads are not covered by the forensic software so vigilance by all staff is needed when children are using the equipment.**
- **Should an incident occur on the ipad the normal procedure of notification would begin.**
- Training updates are now provided by interested staff from the Local Authority Schools, Consortia cluster groups, as and when needed, which are at an additional cost.

Procedure for the Use of Securus Forensic Software

- All staff of the schools must sign an acceptable user policy for the internet as part of their induction.
- All stakeholders including pupils in the school will be made aware of the Securus monitoring system and its monitoring function.
- Violations will be scanned for concerns by a member of the office staff at the schools and if necessary report any violations causing concern to the Heads of School.
- Patterns of violations will be looked for by office admin staff weekly.
- Random selection of the violations will be drilled down to access the offending website/ application
- Where violations are listed to a particular machine, discussions will take place with the staff to clarify the use of the site /applications.
- Where violations are listed to an area e.g. computer suite discussions will take place to discover who was using the computers and possible explanations.
- If the Heads of Schools are unhappy with explanations discussions will take place with the Executive HT.
- Disciplinary procedures will be followed with both staff and pupils involving parents of children where necessary.
- Violations will be archived with Securus and so can be used as evidence.
- Heads of School will sign the dated monitoring sheet regularly.
- At present ipads in school are not covered by the forensic system as there is no facility to do this – as a result staff must be extra vigilant when these are in use with the children. This will be considered at the next contract renewal point.

Procedure for the Protection of Data in Annual School Reports

- Annual written reports will be stored securely in the most appropriate place for each school.
- If staff's wish is to store written reports on a hard drive then the laptop/PC must be encrypted.
- Those members of staff wishing to use a school laptop for the reports at home must sign a school short term loan agreement available from the office and the laptop they take out of school must be encrypted. See agreement for further details.
- If copies of reports are needed for any reason then the office will print these off using the encrypted pen drives.

E-Mail

- Pupils/staff may only use appropriate e-mail accounts on the school system.
- All staff have access to an online account and must ensure that this is only used for the benefit of their professional role at their school.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments unopened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- All staff will only give the school e-mail address to parents and ***not*** their internal personal email address.
- **Staff must not share passwords.**

Published Content and the School Website

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The Heads of School will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Staff must ensure that parents'/carers' wishes are adhered to regarding photographic images published on the school's website. The schools' offices have a list of that information.

Publishing Pupil's Images and Work

- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Signed permission from parents or carers will be obtained before photographs of pupils are published on the school website. This is obtained on entry to the school in the Reception class. If parents wish to change their mind it is their responsibility to inform the school
- Work can only be published with the permission of the pupils and parents / carers.
- Pupil image file names will not refer to the pupil by full name.
- Parents are clearly informed of the school policy on image taking and publishing. This happens on induction to school.
- We try to always use group photographs rather than full faced photos of individual children.
- ***More detailed information on the use of photographs can be found in the 'Policy for Photographs and Images of People in School'***

Passwords

Passwords are becoming increasingly more important.

- They enable secure personal use of a site for adults.
- They reduce the risk of children using another child's website access.
- Staff must create personal passwords for all log ins to the servers in their school.
- Staff hold the responsibility of ensuring that no-one else can log in to their accounts.
- Staff must not share passwords and good practice is to regularly change those passwords.
- Children will have simplified versions of user names and passwords so some vigilance of logging into and off websites and accounts on the server is needed.
- For visitors to school a generic account is to be used with a password –this will be monitored by Securus so it will be possible to trace the users.

Social Networking and Personal Publishing

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- The School and Local Authority block access to social networking sites.
- Twitter –the mini blogging site, is a method of communication used by all the schools but it is only an external feed from the website-no replies can be made by users of this technology.
- All feeds are made by staff and photographs permissions apply.
- Any class /school blogs will be monitored by the senior staff and the class teacher and items only published when satisfied that the content secures safety for our children.
- Children will be made aware that once an item is published, even when deleted, it remains on the internet and is never removed.
- School staff, Governors, pupils, parents /carers will be advised that photographs taken at school events are for personal use only and are not to be published on social networking sites.
- The school will remind parents that social networking sites have an age entry of 13 and above, so our primary school pupils should not have their own accounts.
- We are aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments. We would inform parents if concerns are raised in school.
- Pupils and parents/carers will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils by class teachers /Senior Leadership staff as incidents occur, or, on occasions, when ICT is being discussed as a tool for teaching and learning for example at Meet and Greet evenings in the Autumn term
- All staff of our Federation have signed and accepted Wigan Council's Social Media Policy- this is used in the induction procedure to our schools and is available from the school offices - it gives more detail on acceptable use of social media sites for school employees when not at work regarding issues at work.

Managing Filtering

- The School will work with Wigan Local Authority and Agilysis Filtering services.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-Safety co-ordinator, which will be logged and possibly reported to Agilysis. This facility will then block the site so pupils can no longer enter the site. The school office has the contact name and telephone number.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by engineers.

Managing Skype and Face Time Facilities

- Skype and FaceTime should use the educational broadband network to ensure quality of service and security and only be used on School purchased equipment.
- Pupils must ask permission from the supervising teacher before making or answering an on- line call.
- Skype and FaceTime use will be appropriately supervised for the pupil's age.
- External IP addresses should not be made available to other sites. contact information
- Skype and FaceTime should not be put on the school website.
- The equipment must be secure and if necessary locked away when not in use.
- School equipment should not be taken off the premises without permission.
- A loan form must be completed in the event of a member of staff wanting long term loan of equipment.
- All Skype and FaceTime sessions **must** be logged in a book kept with the facility

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and an informal risk assessment will be carried out before use in school is allowed.
- We should note that technologies, such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Pupils are not allowed mobile telephones in school unless they are in Y5 or Y6 and their parents have sought permission from the school to say that it is needed on the way to/ from school to keep the child safe.
- If a mobile phone is found in school then it will be taken to the school office safe where it will be turned off and handed to a responsible adult at the end of the day.
- Games stations are allowed, at present, for use in before and after school clubs and on occasions, at the discretion of individual class teachers, for example on the last day of the Summer term children may be allowed to bring them in from home as a reward. However it has to be stressed to parents that if they allow children to bring expensive items into school it is at their own risk and the school cannot be held responsible for damage or loss.
- Staff will not use mobile phones to take pictures on trips.

- ***Staff will not use mobile phones during lesson times and phones must not be used for the taking of any pictures in school.***
- The appropriate use of further applications will be discussed as the technology becomes available within the school.
- All photographs of children taken during school hours will be on school purchased digital cameras. No personal cameras are allowed to be used in school by staff.
- Trainees also taking photographs of pupils are only to use school purchased cameras.
- All staff will be issued with the Social Media Policy and asked to sign to say that they accept it in full.
- No staff member must have any child as a 'friend' on any social media site that could compromise their professionalism.

Protecting Personal Data

- Personal Data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4 POLICY DECISIONS

Authorising Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems. This will be held by the Heads of School as part of the safeguarding procedures.
- Parents will be asked to sign and return a consent form. This is completed on formal entry to the school.
- Any person not directly employed by the school will be asked to sign an 'Acceptable use of school ICT resources' before being allowed to access the internet from school site during induction.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network.
- Neither the school nor Wigan Local Authority can accept liability for any material accessed, or any consequences of internet access.
- Senior staff with all members of the staff will audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of E-Safety Policy is appropriate and effective.

Handling E-Safety Complaints

- Any complaint about staff misuse must be referred to the Executive Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure (see School's Complaints Policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet during appropriate meetings during the school year.

5 COMMUNICATION of E- SAFETY

Introducing the E-Safety Policy to Pupils

- E-Safety rules will be posted in all rooms in child friendly language where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up during lessons and assemblies.
- E-Safety training will be embedded within the Computing Schemes of Work.
- Safer Internet Day in February of each year will be used to highlight the importance of e-safety across all areas of school life.
- Opportunities for the education of parents/carers in E-Safety will also be taken when appropriate.

Staff and the E-Safety Policy

- All staff will be given the School E-Safety policy and its importance explained.
- They will sign to say they have read it and accept it in full.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor Internet use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will never use a search engine with the data projector on unless previously prepared.
- We do allow Google to be used in a safe manner.
- Health and Safety including E-safety is an agenda point at every staff meeting including TA meetings.

Enlisting Parents' and Carers' Support

- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website and during appropriate meetings during the year.
- The school will ask all new parents to sign the parent / pupil internet agreement when they register their child with the school or at the pre - entry induction evening.

Thank you to Kent County Council for their assistance in creating this policy.

6 And finally ……..

'It is our responsibility to empower our pupils with the skills to promote safe and responsible behaviour in using technologies both at school, home and beyond.'

Our view is consistent with that of Dr Tanya Byron

"***Children and young people need to be empowered to keep themselves safe- this isn't just about a top down approach. Children will be children-pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach pupils to swim"***