ALVANLEY
MANLEY
Federated Primary Schools

e-Safety Policy

based on

Cheshire Shared Services

e-safety policy

Guidance for Schools

DRAFT – REVIEWED AT MEETING 22/02/2010

The Digital Age**:** where a wide range of different media content can be accessed through a wide range of devices in a wide range of places!
And the technology continues to march on, and with it the range of content that is available. Your phone is no longer just a phone. It will take photographs, play music and probably connects to the internet. Your computer is not just for writing letters on or working out your finances, it is for playing games, watching films, listening to music and socialising with your 'friends'. The games console now provides fascinating, and sometimes frightening, realistic imagery of imaginary worlds in which you can become a part and mix, via the internet, with likeminded individuals. And this connectivity, the ability to link up with other people electronically is now wireless and, therefore, we are always 'on' wherever we are. Young people are probably more 'on' than their parents, carers and teachers. This is their world. They are often called digital natives, naturally assimilated into this connected digital world. This does not, however, mean that they naturally understand and have the wisdom to behave appropriately and safely in this connected digital world. It is up to us as adults in general, and parents, carers and teachers in particular, as digital immigrants, to understand their world as much as we can so that we can help and support them in developing their understanding and wisdom.

This eSafety policy is one step on that road, outlining the steps schools and settings can take to support our development and understanding of eSafety. It outlines common issues and also provides a matrix to support you in dealing with incidents. We commend this to you and encourage you to take those steps to help support and protect our young people by making them digitally aware and able to start making their own decisions and take personal responsibility for staying safe on-line.

We recognise that within our schools and settings we can try to lock out the wider world and keep young people safe but it is important for us to teach them about the outside world, the world when they go home and log on in their bedroom, the world that is in their pocket via their phone and the world they experience on their games console. We need to ensure that we provide them with the resilience and tools to effectively cope with the 'inappropriate' material or contact that they may become exposed to at some point in their 'on life' lives. This is education for life. We need to teach our children so that they can know what to do and who to talk to keep themselves and others safe.

E-Safety: The Rationale

E-Safety encompasses the use of new technologies, internet and electronic communications such as Learning Platforms, mobile phones, Video Conferencing, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their on line experience.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from an approved Internet Service Provider using suitable filtering.
- National Education Network standards and specifications.

Schools E-Safety Audit

This short audit will help schools to focus upon areas where further consideration or actions may be required when reviewing E-safety within their school.

The school has an e-Safety Policy that complies with Cheshire Children's Services and / or Becta guidance.	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at	
And for parents at	
The Designated Child Protection Coordinator is	
The e-Safety Coordinator is	
How is E-Safety training provided?	
Is the Think U Know training being considered?	Y/N
All staff sign an Acceptable ICT Use Agreement and any subsequent revisions.	Y/N
Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement on entry to the school and any subsequent revisions.	Y/N
Rules for Responsible Use have been set for students and are regularly updated.	Y/N
These Rules are displayed in all rooms with computers.	Y/N
Internet access is provided by an approved educational Internet Service Provider and complies with DCFS requirements for safe and secure access.	Y/N
The school filtering policy has been approved by SMT.	Y/N
An ICT security audit has been initiated by SMT, possibly using external expertise.	Y/N
School personal data is collected, stored and used according to the principles of the Data Protection Act.	Y/N
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SMT.	Y/N
Staff have received training in the use of filtering / auditing software and are aware of the processes involved in disclosure.	Y/N

1.1 Writing and reviewing the e-safety policy

*Our school's e-safety co-ordinator is*________________________________

- Our e-Safety Policy has been written by the school, building on the Cheshire e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors and is available for parents online or as a hard copy form school.
- The e-Safety Policy was revised by: … … … … ……………………
- It was approved by the Governors on: … … ………………………….

  and is due for review on...

1.2 Teaching and learning

1.2.1 Why Internet use is important

- The Internet is an essential element in 21st century 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 staff and pupils.

1.2.3 Internet use will enhance learning

The school Internet access will be designed expressly for pupil and family use and will include filtering appropriate to the age of pupils.

Pupils and families 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

1.2.4 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.

1.3 Managing Internet Access

1.3.1 Information system security

School ICT systems and security will be reviewed regularly.

Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily.

We have adopted Cheshire West and Chester security standards as laid out in

1.3.2 E-mail

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.

- 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.

1.3.3 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.

1.3.4 Publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

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 photographs of pupils are published on the school Web site.

1.3.5 Social networking and personal publishing

The school (or should this be)LA? will block/filter access to social networking sites.

Newsgroups (what is newsgroup) 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 may be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Staff are advised that they should consider the consequences and possible repercussions of any information that they make available online, for example on a social networking site. Particular care should be taken in the posting of photographs, videos and information related to the school, school life, staff and pupils.

What should staff use of laptop both within and outside of school hours be? E.g Tesco's orders etc.

Don't put children's photos on phone.

Members of staff need to consider and be aware of the way that information is posted and understand that once it is there it is very difficult, if not impossible to remove it. An understanding of the tagging of photographs and video needs consideration. Even if I don't put a picture up of myself somebody else can and tag it with my name and a comment. Sometimes this may not be a picture I would wish to share with the world, particularly if the site on which it is posted is accessed by pupils / students. These are wider societal issues but their impact will be felt in schools, particularly around privacy and what may be deemed to be appropriate conduct for professionals working with children.

1.3.6 Managing filtering

The school will work with the LA, DCFS 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 who should be known to all members of the school community.

Filtering websites limits access within the school to generally appropriate sites. Filtering can never be a 100% accurate and should be supported by appropriate supervision for the age of pupils'. It works by categorising websites and blocks inappropriate category's such as pornography and gambling. The Local Authority, as the Internet Service Provider, includes filtering at a County level. If sites are blocked there is a mechanism to release sites on approval by the Advisory team. Where schools find sites or content that is inappropriate they should contact Help Desk on 01244 97400 and ask for the site to be blocked.

Securus

1.3.7 Managing video conferencing

IP video conferencing 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 video conference call.

Video conferencing will be appropriately supervised for the pupils' age.

Video conferencing is an increasingly useful technology, particularly at Secondary level, where a Video Conferencing suite may be used. Less sophisticated technologies using web cams will become more popular as internet functionality increases and new uses are identified. Video conferencing is very resource heavy and can have a significant impact upon the performance of the network. Technologies such as Skype may be considered appropriate for home use are not to be encouraged within the schools' network. Learning platforms are likely to incorporate simple point to point video conferencing as part of their communication tools.

1.3.8 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.

- Staff mobile phones will only be used during lessons or formal school time in the case of emergency. The sending of abusive or inappropriate text messages is forbidden.

  Staff will not use personal equipment or non school personal electronic accounts when contacting students. They will be issued with a school phone where contact with pupils is required.

- If a child needs to bring a mobile phone into school it MUST be stored in the school office during the school day

It is inevitable that technology will continue to develop and young people will continue to have an appetite to explore and find uses for it. It is important that we keep up to date with new technologies and understand how they are used and potentially abused. It is ultimately simple to ban a technology but not necessarily the most effective method in educating young people how to use it safely or appropriately.

1.3.9 Protecting personal data

Any personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff need top have encrypted memory sticks and we are investigating the encrypting of information on laptops.

1.4 Policy Decisions

1.4.1 Authorising Internet access

All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.

All students and their parents must read and agree to the 'Students' Safety Rules'.

Parents will be asked to agree to and return a consent form with respect to the 'Students' Safety Rules'.

The school will keep a central record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

Within the Primary school access to the Internet will be supervised. Lower down the school access to specific, approved on-line materials.

All users of ICT resources within the school establishment must agree to the acceptable use agreement. The school should keep an up to date record of all agreements which may be by signed paper copies or completion of an electronic form. It is the head teacher's responsibility to ensure that the record is kept up to date and we strongly recommend a centrally kept record for both staff and pupils / students so that it can be easily referred to. If your school has a learning *platform in place it is worth using a form or survey tool to gather the data electronically. An additional benefit of this methods is a response can be required for each question.*

1.4.2 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 local authority can accept liability for the material accessed, or any consequences of Internet access.

The school will regularly audit regularly ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

1.4.3 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 or Chair of Governors.

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.

1.5 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

E-safety rules will be posted in all classrooms and discussed with the pupils regularly.

Pupils will be informed that network and Internet use will be monitored.

1.5.2 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.

1.5.3 Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy by letter and on the school Web site.

Ask Redtop re individual logons

Appendix 1: Internet use - Possible teaching and learning activities

Activities	**Key e-safety issues**
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. The Learning Platform.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.
Communicating ideas within chat rooms or online forums.	Only chat rooms contained with the schools Learning Platform and linked to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.

Date Authored	February 2010
Date Ratified By Governors	
Date for Review	Autumn 2017