- Supervises children and young people's use at all times and is vigilant in the areas where young people have more flexible access;
- We use an appropriate and approved filtering system which blocks harmful and inappropriate sites;
- We have added additional user-level filtering, and can be appropriately adapted. Websites to be used with children and young people should be previewed by staff.
- If raw image searches are used staff vigilance is crucial
- Computer use is monitored and logged on all school equipment both inside and outside of school.
- Manages access to Chat rooms and social networking sites and recommends those that are part of an educational network or approved Learning Platform;
- Has blocked children and young people's access to music download or shopping sites – except those approved for educational purposes.
- Requires students to individually sign an e-safety / acceptable use agreement form which is fully explained.
- Requires all staff, on induction, to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse. Keeps a record, of any bullying or inappropriate behaviour for evidence in line with the school behaviour policy;
- The named child protection officer for in E safety is Mr M Allison ;
- Ensures parents provide consent for their child to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement.
- Makes information on reporting offensive materials, abuse / bullying etc available for children, young people parents and carers and staff;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information to the school website is restricted to the Assistant Headteacher, website technician and the ICT curriculum manager. All teachers can upload information to the VLE.
- The school website complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the website is the school address and telephone number. Home information or individual e-mail identities will not be published;

- Photographs published on the web do not have full names attached;

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are only able to publish to their own 'safe' web-portal
- Pupils are taught about how images can be abused in their eSafety education program;

Student data and personal information

The school is responsible for the safeguarding of student data and information. When data is exported to external organisations for processing it is always done so in an encrypted manner.

Staff are informed not to take pupil personal information out of School. If they access pupils data electronically this must be done through SIMS remote, which is password protected and must be accessed through the School website.

Social networking and personal publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: facebook, blogs, wikis, Instagram, tumblr, MySpace, Snap Chat, Piczo, Windows Live Spaces, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- The schools will block/filter access to social networking sites.
- Newsgroups 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 and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Radicalisation

- Protecting children from the risk of radicalisation (PREVENT) is seen as part of schools' wider safeguarding duties, and is similar in nature to protecting children from other harms (eg drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences. The school is aware of the increased risk of online radicalisation, as terrorist organisation such as ISIS seek to radicalise young people through the use of social media and the internet. This is managed as part of this e-safety policy, linked with the safeguarding policy.

Mobile Phones

- The School also has a mobile phone policy that can be found on the website.

http://www.mcauley.org.uk/index.php/component/phocadownload/category/40-policies-a-information