ORCHARD PRIMARY SCHOOL

Computing and e-Safety Policy

Computing Policy

Introduction

The use of information and communication technology is an integral part of the national curriculum and is a key skill for everyday life. Computers, tablets, programmable robots, digital and video cameras are a few of the tools that can be used to acquire, organise, store, manipulate, interpret, communicate and present information. At Orchard Primary School we recognise that pupils are entitled to quality hardware and software and a structured and progressive approach to the learning of the skills needed to enable them to use it effectively. The purpose of this policy is to state how the school intends to make this provision.

Aims

- Provide a relevant, challenging and enjoyable curriculum for computing for all pupils.
- Meet the requirements of the national curriculum programmes of study for computing.
- Use computing as a tool to enhance learning throughout the curriculum.
- To respond to new developments in technology.
- To equip pupils with the confidence and capability to use computing throughout their later life.
- To enhance learning in other areas of the curriculum using computing.
- To develop the understanding of how to use computing safely and responsibly.

The national curriculum for computing aims to ensure that all pupils:

- Can understand and apply the fundamental principles of computer science, including logic, algorithms, data representation, and communication
- Can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems.
- Are responsible, competent, confident and creative users of information and communication technology.

Rationale

The school believes that computing:

- Gives pupils immediate access to a rich source of materials.
- Can present information in new ways which help pupils understand access and use it more readily.
- Can motivate and enthuse pupils.
- Can help pupils focus and concentrate.
- Offers potential for effective group working.
- Has the flexibility to meet the individual needs and abilities of each pupil.

Objectives

Early years

It is important in the foundation stage to give children a broad, play-based experience of computing in a range of contexts, including outdoor play. Computing is not just about computers. Early years learning environments should feature computing scenarios based on experience in the real world, such as in role play. Children gain confidence, control and language skills through opportunities to 'paint' on the whiteboard or programme a toy. Recording devices can support children to develop their communication skills. This is particular useful with children who have English as an additional language.

Key Stage 1

By the end of key stage 1 pupils should be taught to:

- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions
- Write and test simple programs
- Use logical reasoning to predict and computing the behaviour of simple programs
- Organise, store, manipulate and retrieve data in a range of digital formats
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

Key Stage 2

By the end of key stage 2 pupils should be taught to:

- Design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
- Use sequence, selection, and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs
- Use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs
- Understand computer networks including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration
- Describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely
- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Roles and Responsibilities

The senior leading team is primarily responsible for monitoring all computing planning within the school on a weekly basis, although the computing subject leader monitors planning. The computing subject leader is responsible for informing the rest of the staff about new developments and, where appropriate, for organising or providing appropriate training. The computing subject leader advises colleagues on managing equipment and software in the classroom. They are also expected to manage resources in the computing suite and ensure the central resources are being used efficiently and effectively. The computing subject leader is required to manage the budget responsibly. The computing subject leader acts as a liaison point between the computing technicians and the teaching / non teaching staff. The computing subject leader will report to the Head Teacher and computing Governor, any areas of concern or good practise, as and when required.

Equal Opportunities

As a school we recognise the advantages of using ICT with all pupils, including those children with Special Educational Needs (SEN).

The school promotes equal opportunities for computer usage. To do this we will:

- ensure that all pupils have frequent access to computing equipment
- provide a wide range of software as possible
- provide software that allows access for SEN pupils
- obtain software that supports more able learners, where possible
- take account of the language skills of all our pupils
- use software that is not gender based but promotes positive images of computer use by both girls and boys
- encourage all staff to become more confident and competent in their use of ICT
- be aware of cultural diversity when selecting software to be used.

Planning

As the school develops its resources and expertise to deliver the computing curriculum, modules will be planned in line with the national curriculum and will allow for clear progression. Modules will be designed to enable pupils to achieve stated objectives. Pupil progress towards these objectives will be recorded by teachers as part of their class recording system. Staff will follow medium term plans with objectives set out in the national curriculum and use the same format for their weekly planning sheet.Teachers are expected to plan for computing across the curriculum and this is recorded on all planning where appropriate and highlighted pink.

Teaching and Learning Styles

New skills will be demonstrated to the children as a whole class. The majority of the input will be carried out in the computing suite and can be followed up in the classroom. However, with the introduction of interactive whiteboards in all

classrooms it makes it easier to teach these skills within the classroom context. The computing subject leader will observe lessons, as part of a learning walk, to look at the range of teaching styles that are employed to develop computing capability. These teaching styles include: group work of mixed and similar ability, individual work and whole class teaching. Teachers' planning may also include opportunities for work away from the computers to complement the computing activities.

Record Keeping and Assessment.

A key factor in the success of the new medium plan will be that teachers rigorously assess pupils' prior learning so that they are enabled to build on this and make good progress, learning how to apply skills across other learning. Teachers have also been advised to consider how to cluster skills appropriately so that pupils are aware of the context in which they can apply their learning.

Teachers will record a child's attainment at the end of each lesson on the computing assessment sheet. This will be monitored by the computing subject leader. The sheet will be passed on to the next teacher. At the end of each lesson, if relevant, children or staff will be required to save the work for each child under the 'u' drive, creating a folder for each year group. This will act as a portfolio which staff can access to look at the progression of the children. Parents are kept informed of their child's progress via an annual report, written by the class teacher, as well as verbal feedback during parent evenings.

Organisation of Resources

Hardware: Staff needs to ensure that their computer and laptops in the classroom, as well as peripherals (printer, mouse etc) in the classroom are kept in working order. If there is a problem they need to record on an error sheet kept in the computing suite and, if urgent, let the computing subject leader know. Who will, in turn, let the technician know. Staff are also required to maintain a safe and tidy working environment with regards to computer equipment, making sure all wires are safely tucked away. Staff need to identify technical errors in the computer suite by using the same process. Training will be given, as and when required, to keep staff updated on dealing with faults. Staff also has access to other peripherals (including digital cameras, digital video cameras, digital microscopes etc).

At present there are 30 stand alone computers in the computing suite and each class will have weekly timetabled sessions. Timetabling of the computing suite takes place at the beginning of every school year and staff are expected to sign up for at least one session, although staff are encouraged to use the computing suite for other areas of the curriculum. When computing is used to support other curriculum areas it should be at an appropriate level within the children's capabilities and should not involve the teaching of new skills. The timetable will be placed on the wall in the computing suite and, aside from the previously allocated sessions, staff can sign up as and when required. Since 2009 each class has been allocated 6 laptops with the Foundation Stage sharing 6 between them. These need to be used to enhance teachers cross curricular links in computing

and make it easier to access computing programmes/technology to enhance the teaching and learning.

Software: Some software will be installed on to the class computer or laptops if the number of licences purchased allows. The licences are stored in a folder in the computing suite or with the computing subject leader. There is also a central store, kept in the locked cupboard in the computing suite, which contains cross-curricular or multi year group software. A list of all software purchased and used whether in the computing suite or in individual classrooms will be kept and updated by the computing subject leader. Staff that purchase software for their curriculum area are expected to let the computing subject leader know so it can be recorded on the list and a copy of the licence needs to be provided.

Networking: Currently all computers in the computing suite are networked, along with all laptops and stand alone computers located in the classrooms and SEN rooms. All classrooms have access to the Internet which is supported by LGfL. Laptops from the laptop trolley can use a wireless connection to connect to the network providing the networking box has been connected. When working in the computing suite the laptops can be used wirelessly although connecting the network cable will ensure speed.

Outside support

The school is currently working with a company called ATS who provide support for 3 hours every Tuesday and can also be contacted by phone at other times to give advice. They provide a technician who works closely with the computing subject leader, maintaining the computers in the computing suite and classrooms, as well as working on faults identified by the staff.

ICT training may be provided by outside agencies to help staff with their Continuing Professional Development. The computing subject leader will be responsible for identifying the needs of the staff and providing arrangements for adequate training.

Security

There is an alarm system fitted throughout the building. The computer suite is made secure at night as part of the site manager's daily routine. Each piece of hardware is inscribed with the name of the school and the postcode. All smaller peripherals should be locked away or kept out of sight wherever possible. Laptops should be stored somewhere out of sight or locked away wherever possible when left in the building during the holiday's or weekend.

The computers use 'Winsuite' – a security system allowing children and staff to access their work through a password. The management system has a separate password which only the Head Teacher, computing subject leader and technician have access to.

Use of computing will be in line with the school's 'acceptable use policy'. All staff, volunteers and children must sign a copy of the schools AUP.

- Parents will be made aware of the 'acceptable use policy'.

- All pupils and parents will be aware of the school rules for responsible use of computing and the internet and will understand the consequence of any misuse.
- The agreed rules for safe and responsible use of computing and the internet will be displayed in all computing areas.

Use of the Internet

There is an Internet Access Policy in place. This is an agreement between the school, pupils and parents to ensure that where pupils are accessing the internet appropriate measures will be taken to prevent them from accessing inappropriate material. Currently the LEA filters the sites that the children can have access to. If children do gain access to inappropriate material the member of staff should inform the computing subject leader and record it in blue file, locked in grey cupboard in computing Suite. The computing subject leader will inform the LEA, if appropriate.

Orchard Primary School
E-Safety Policy

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to the ICT leader.
The E-Safety Policy relates to other policies including those for ICT, bullying (found in behaviour management) and for child protection.
The e-Safety co-ordinator at Orchard is the Head Teacher as e-Safety and child protection overlap.
Our E-Safety Policy has been written by the school, building on government guidance. It has been agreed by staff and approved by governors.
It was approved by the Governors
on:……..
The next review date is Spring Term 2017.

Technical and Infrastructure approaches

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;
- Uses individual, audited log-ins for all users - the London USO system;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Only uses the LGfL service for video conferencing activity;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Provides staff with an email account for their professional use, *LA* email and makes clear personal email should be through a separate account;
- Uses teacher 'remote' management control tools for controlling workstations viewing users / setting-up applications and Internet web sites, where useful;

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupil's age.

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 staff and pupils.

Internet use will enhance learning

- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are 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.

Policy and procedures:

This school:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the teacher. Our ICT leader logs or escalates as appropriate to the Technical service provider or LGfL as necessary;

- Requires pupils to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programmes;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides e-safety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

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.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, 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.
- Work can only be published with the permission of the pupil and parents/carers.

<u>Education and training:</u>

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher.

- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Makes training available to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents, including:
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home;

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.
- The senior leadership team 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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means id forbidden.

Protecting personal data

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

Handling E-safety complaints

- Complaints of Internet misuse will be dealt firstly with the ICT subject leader who will report to a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- 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 schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the E-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- An e-safety display will be in the ICT suite.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

Staff/Adults and the E-Safety policy

- All Staff/Adults will be given the School E-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School E-Safety policy on the school Web site.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

Appendix 1

Internet policy and procedures: background information

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation.

Surfing the Web

Aimless surfing should never be allowed. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the Internet?"

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger pupils 'searching the Internet'.
Pupils do not need a thousand Web sites on weather. A small selection will be quite enough choice, and as with other resources, the teacher needs to have checked and selected them so they are appropriate for the age group and fit for purpose. Favourites / bookmarks are a useful way to present this choice to pupils. Teachers' web site selections for various topics can be put onto a topic page on the Learning Platform so pupils can, access out of school, from home etc. Some schools put links on their school web site, although there may even be difficulties here. Hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing. Therefore, sites should always be previewed and checked, and work for children is best located on the closed Learning Platform.

Search Engines
Some common Internet search options are high risk, for example 'Google' image search. Some LAs and Councils block this. Others keep it unblocked because it can be a useful tool for teachers looking for images to incorporate in teaching. Where used – it must be with extreme caution. Google image search can be set-up to run in 'safe' mode although this is not fully without risk. Talk to your network manager or Technical support provider about this. LGfL guidance is available on the safety site.
Images usually have copyright attached to them which is an issue commonly overlooked but a key teaching point to pupils and staff.

Collaborative Technologies
There are a number of Internet technologies that make interactive collaborative environments available. Often the term 'Social networking software' is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcast sites (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop racy and presentations skills, helping children consider their content and audience. Schools are best protected by using the social collaboration tools within the school's Learning Platform, such as the London MLE..
Blogs: A School may want to use them as a method of online publishing, perhaps creating class blogs, or to creatively support a specific school project. A 'safe' blogging environment is likely to be part of a school's Learning Platform or within LGfL /LA provided 'tools'.
Webcams and Video Conferencing
Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. LGfL has a number of nature cams showing life inside bird boxes for example and a plethora of weather cams across London providing detailed real-time weather data. Webcams can also be used across London for streaming video as part of a video conferencing project.
Video conferencing provides a 'real audience' for presentations and access to places and professionals – bringing them into the classroom. For large group work high quality video conferencing hardware equipment is required to be plugged into

the network. LGfL, and the other national regional grids for learning, have made an agreement with JVCS (the Janet Videoconferencing Service) to host calls. All conferences are therefore timed, closed and safe. This is a service that is included in LGfL 2. Advice can be found here
http://www.lgfl.net/SERVICES/CURRICULUM/Pages/WeatherStations.aspx
http://www.lgfl.net/learningresources/VideoConferencing/Pages/Home.aspx
Pupils can search on the Internet for other webcams - useful in subject study such as geography (e.g. to observe the weather or the landscape in other places). However, there are risks as some webcam sites may contain, or have links to adult material. In schools adult sites would normally be blocked but teachers need to preview any webcam site to make sure it is what they expect before ever using with pupils.
The highest risks lie with streaming webcams [one-to-one chat / video] that pupils use or access outside of the school environment. Pupils need to be aware of the dangers.

Podcasts
Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments such as the LGfL. Podcast central area.
http://www.lgfl.net/SERVICES/CURRICULUM/Pages/Podcasting.aspx
Chatrooms
Many sites allow for 'real-time' online chat. Again, children should only be given access to educational, moderated chat rooms. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school where they may access chatrooms such as www.teenchat.com, www.habbohotel.co.uk, www.penguinchat.com
Sanctions and infringements
The school's Internet e-safety / Acceptable Use policy needs to be made available and explained to staff / Governors, pupils and parents, with all signing acceptance / agreement forms appropriate to their age and role. The school needs to have made clear possible sanctions for infringements.
Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on school computers, the matter should be immediately referred to the Police. There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence.

Appendix 2

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour.

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. (All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process: **https://www.thinkuknow.co.uk/parents/browser-safety/**

Summer Term 2014
To be reviewed Spring Term 2017