Online Safety Policy

Date of Policy: Summer 2017
Policy Review date: Summer 2018

Signed:
Headteacher:

Signed:
Chair of Governors:

CONTENTS

1. INTRODUCTION

School Online Safety Policy

1.1   Writing and reviewing the Online Safety Policy

- The Online Safety Policy relates to other policies including those for Computing and for child protection.
- The school has appointed an Online Safety Officer and Link Governor. (*See appendix 6*)
- Our Online Safety Policy has been agreed by the Senior Management Team and approved by governors.
- The Online Safety Policy will be reviewed every 1 year.

1.2   Teaching and learning

1.2.1   Why Internet use is important

- The Internet is an integral 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.

1.2.2   Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils by Smoothwall Filtering and Safe Guarding Package from WES.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2. AIMS AND OBJECTIVES

- To provide staff with the key information to deal with online safety issues in a safe and effective manner.
- To ensure that staff have the ability to deal with content, contact and conduct issues on line.
- To provide staff with a point of reference when dealing with online safety issues.

3. EQUAL OPPORTUNITIES

- All children should have equal access to the use of the Internet.

- Further information on equal opportunities and special needs is given in the relevant school policies.

4. ORGANISATION

4.1   Curriculum

- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, (eg using search engines) staff should be vigilant in monitoring the content of the websites the pupils visit.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- KS1 - Pupils should be taught to: use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- KS2 - Pupils should be taught to: use technology safely, respectfully and responsibly; recognise acceptable/ unacceptable behaviour; identify a range of ways to report concerns about content and contact.
- Carl's Online Safety Team (COST) Cadets meet each half-term.

4.2   Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Online Safety Officer, who then must report it to Warwickshire ICT Development Service. Tel: 414100

- The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

4.3   Managing Internet Access

4.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection is installed and updated regularly by Launch Systems.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an additional level of protection through its deployment of Warwickshire ICT Development Service monitored system called 'Policy Central'. This software monitors text appearing on the screen and keyboard input, identifying the use of words that are included on a list of 'banned words'. The software captures the screen, identifying machine and user details so appropriate action can be taken.

4.3.2 E-mail

- Pupils currently do not use e-mail accounts on the school system.

4.4   Passwords

All users will be provided with a username (and KS2 password):

Reception - username=r and no password
Year 1 - username=year 1 and no password
Year 2 - username= children's name and no password (introduced by the Summer term)
Year 3 - username=children's name and password =random letters and numbers
Year 4 - username=children's name and password =random letters and numbers
Year 5 - username=children's name and password =random letters and numbers
Year 6 - username=children's name and password =random letters and numbers

- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

4.5   Publishing

4.5.1   Published content and the school website

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.5.2   Publishing pupils' images

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.
- Written permission from parents or carers will be obtained before photos of pupils will be used for display and educational use, the portal, publications, on the school website by us, by the Local Authority or by local newspapers. (See appendix 1)

4.5.2 .1 Publishing pupils' names

- Recordings that are published will only use pupils' first names.

4.5.3   Social networking and personal publishing

- Social networking sites, chat rooms and newsgroups are blocked unless a specific use is approved.
- The school Twitter account is only used by staff following strict procedures.
- Pupils and parents are advised that the use of social network spaces outside school may be inappropriate for pupils. (Some parents have strong positive views and it may be necessary to consider carefully how advice is given) See 4.8.3
- Pupils are advised never to reveal personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

4.6   Managing filtering

- The school will work in partnership with the Warwickshire ICT Development Service to ensure filtering systems are as effective as possible.
- The Online Safety Officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

4.7   Protecting personal data

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

4.8   Handling Online Safety complaints

- Any complaints of Internet misuse are dealt with initially by the Online Safety Officer and/or Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any complaint about parent/community misuse must be referred to the Headteacher.

- Any complaint about the Headteacher must be referred to the Chair of Governors.
- Any complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

4.9   Community use of the Internet

- The school is sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Wider community use will fall under the same obligations as staff use. Using Appendix 2a

4.10   Communications

4.10.1 Introducing the Online Safety Policy to pupils

- Carl's Online Safety Team (COST) Cadets meet each half-term.
- Rules for responsible ICT use are posted in all networked rooms. (See appendix 5)
- Pupils are informed that Internet use will be monitored.
- Regular Online Safety training will be provided to raise the awareness and importance of safe and responsible Internet use.

4.10.2 Staff and the Online Safety Policy

- All staff are given the School Online Safety Policy and its importance explained.
- All staff read and sign the School Online Safety Agreement Form each September.
- Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

4.10.3 Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, in the prospectus and on the school web site.
- The need for a parents meeting or information leaflet will be reviewed annually.

5. MONITORING

5.1   Authorising Internet access

- The school maintains a current record of all staff and pupils who are granted Internet access in the WI-FI Agreement File kept in the School Office cupboard.
- All staff must read and sign the acceptable ICT use agreement, 'Online Safety Agreement Form for School Staff', before using any school ICT resource. (See appendix 2)
- Parents sign the 'Online Safety agreement form for parents of Primary aged children'. (See appendix 3)

- Children sign the 'Online Safety agreement form for KS1 / KS2 school pupils (*See appendix 4 KS2/KS1,*)

5.2   Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 WCC can accept liability for the material accessed, or any consequences of Internet access.

- The Online Safety Officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Recording reported events.

- The Headteacher ensures that the Online Safety Policy is implemented and compliance with the policy is monitored.

6. EDUCATION

6.1 Pupils

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's Online Safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

- Online Safety education will be provided through the Computing schemes of work in the following ways:
  o A planned Online Safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
  o Key online safety messages should be reinforced as part of a planned programme of assemblies and PSHE activities
  o Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
  o Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
  o Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
  o Staff should act as good role models in their use of ICT, the internet and mobile devices

6.2 Parents/carers

- Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents often

either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

- The school will therefore seek to provide information and awareness to parents and carers through:
  o Letters, newsletters, website
  o Online safety parent sessions
  o 1-2-1 parent/carer meetings

6.3 Education- extended schools

- The school will offer family learning courses in online safety so that parents and children can together gain a better understanding of these issues. Messages to the public around online safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

6.4 Training- staff

- It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
o A planned programme of formal online safety training will be made available to staff.
o All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
o The Online Safety Officer (or other nominated person) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA / LA and others.
o This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
o The Online Safety Officer will provide advice / guidance / training as required to individuals as required

6.5 Training - governors

- Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / online safety / health and safety / child protection. This may be offered in a number of ways:
o Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
o Participation in school training / information sessions for staff or parents

7. COMMUNICATIONS

7.1 Communication technologies

- A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

7.2 Permitted communication technologies table

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or personal camera devices				x				x
Use of hand held devices eg PDAs, PSPs	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 chat rooms / facilities			x					x
Use of instant messaging				x				x
Use of social networking sites				x				x
Use of blogs		x					X	

- When using communication technologies the school considers the following as good practice:

  o The official school email service may be regarded as safe and secure and is monitored.
  o Users need to be aware that email communications may be monitored
  o Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable,

is offensive, threatening or bullying in nature and must not respond to any such email.

o Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

o Personal information should not be posted on the school website and only official school email address should be used by parents/carers to communicate with staff members

8. RESPONDING TO INCIDENTS OF MISUSE

8.1 Illegal activity

- It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

- Examples of illegal activity could include:
  o child sexual abuse images
  o adult material which potentially breaches the Obscene Publications Act
  o criminally racist material
  o other criminal conduct, activity or materials

8.2 Inappropriate activity

- It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

8.3 Pupils action/sanction table

Pupils   Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Online Safety Officer	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Consideration of further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal		X	X	X	X				
Unauthorised use of non-educational sites during lessons	X								X
Unauthorised use of mobile phone / digital camera / other handheld device			X						X
Unauthorised use of social networking / instant messaging / personal email			X						X
Unauthorised downloading or uploading of files			X						X
Allowing others to access school network by sharing username and passwords	X	X						X	X
Attempting to access or accessing the school network, using another student's / pupil's account	X	X						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
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X			X			X
Continued infringements of the above, following previous warnings or sanctions		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
Using proxy sites or other means to subvert the school's filtering system			X						X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X		X		X			X

8.4 Staff action/sanction table

Staff — Actions / Sanctions

Incidents:	Refer to Online Safety Officer	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X		X		X	X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		X	X			X		X
Unauthorised downloading or uploading of files		X	X			X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X				X		X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules		X	X			X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X			X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X			X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X	X			X		X
Actions which could compromise the staff member's professional standing	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
Using proxy sites or other means to subvert the school's filtering system		X	X			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	X
Breaching copyright or licensing regulations		X	X			X		X
Continued infringements of the above, following previous warnings or sanctions		X	X			X	X	X

9. FUTURE DEVELOPMENTS

9.1   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.

- Mobile phone technology will not be used during lessons or formal school time by pupils.

- Staff must not use their own mobile phone where contact with parents/carers is required. The school mobile phone shall be used, if off-site.

10.　　APPENDICES

Appendix 1

SCHOOL VISITS

We often take the children off site when opportunities arise for the class or individually for certain events. It is important that we gather this information. We will notify you with a separate letter of any trips or visits.

Please indicate your preference for each individual trip, visit or sporting event			
Visit or Event	Please specify for each visit or event		Signed to confirm
Visit to local attractions within walking distance	YES	NO	
Sporting activities off site eg: tag rugby, swimming, cross country at local facilities within walking distance.	YES	NO	

PHOTOGRAPHS

We take lots of photographs in school to celebrate the children's learning. Please can you provide us with information with regard to your preference on how we use these photographs. It is vitally important that we gather this information as Safeguarding Children is paramount to us.

Please indicate for each individual circumstance			
	Please specify for each circumstance when a photograph may be taken		Signed to confirm
Permission for my child to have their photograph taken and have their name printed (NO SURNAME) at the discretion of the school for press reports	YES	NO	
Permission for my child's photograph to appear on the school website	YES	NO	
Permission for my child's photograph to appear on TWITTER	YES	NO	
I agree that any photographs of my child that I take at school events, where photography is allowed, such as Sports Day, Assemblies and productions, are taken on the understanding that I will NOT post them on any Social Media (eg: Facebook) if they include anybody else's child.			
Signed:			Date:
(Parent/Guardian)			

Clapham CARL

Caring - Achieving - Respectful - Learners

Online Safety Agreement Form

For School Staff

- I understand that the network is the property of the school and agree that my use of this network must be compatible with my professional role.

- I understand that the school ICT systems may not be used for private purposes, without specific permission from the Headteacher.

- I understand that use for personal financial gain, gambling, political purposes or advertising is not permitted.

- I understand and agree that the school will monitor my network and Internet use to ensure policy compliance.

- I will respect ICT system security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will not install any software or hardware without permission.

- I will not disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system.

- I will take all reasonable precautions to secure data or equipment taken off the school premises.

- I will report any incidents of concern to the school's Designated Child Protection Staff or Online Safety Officer as appropriate.

- I will ensure that my electronic communications with pupils are compatible with my professional role and cannot be reasonably misinterpreted.

- I will promote online safety with the pupils that I work with and will help them to develop a responsible attitude to ICT use.

- I will respect copyright and intellectual property rights.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed: …………………………………………… Capitals: ………………………

Accepted for School: …………………………… Capitals: ………………………

Date: ………………………………….

This form is valid for the time the staff member is employed at the school and will automatically expire after this time.

Online Safety Agreement Form

For Community Use

- I understand that the network is the property of the school and agree that my use of this network must be compatible with an agreed community use.

- I understand that the school ICT systems may not be used for private purposes, without specific permission from the Headteacher.

- I understand that use for personal financial gain, gambling, political purposes or advertising is not permitted.

- I understand and agree that the school will monitor my network and Internet use to ensure policy compliance.

- I will respect ICT system security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will not install any software or hardware without permission.

- I will not disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system.

- I will take all reasonable precautions to secure data or equipment taken off the school premises.

- I will report any incidents of concern to the school's Designated Child Protection Staff or Online Safety Officer as appropriate.

- I will respect copyright and intellectual property rights.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed: ……………………………………… Capitals: ………………………

Accepted for School: …………………………… Capitals: ………………………

Date: …………………………………….

This form is valid for the period of agreed usage.

Appendix 3

Online Safety Agreement Form
For Parents of Key Stage 2 Aged Children

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter / son to have access to use the Internet and other ICT facilities at school.

I know that my daughter / son has signed an online safety agreement form and that they have a copy of the "12 Rules for responsible ICT use".

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered and monitored service, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their online safety or online behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent / guardian signature: _____

Date: ___/___/___

This form is valid for the period of the time your child attends this school and will automatically expire after this time.

Online Safety Agreement Form

For Primary School Pupils

(See following pages)

Keeping Safe:
Stop, Think, Before you click!

Pupil name: _____

I have read the school's '12 Rules for responsible ICT use'.   My teacher has explained them to me.

I understand these rules are there to help keep me safe, and my friends and family safe.   I agree to follow the rules.

This means I will use the computers, Internet, online communities, digital cameras, iPads, video recorders, and other ICT in a safe and responsible way. I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, they may contact my parent / guardian.

Pupil's signature _____

Date: ___/___/___

This form is valid for the period of the time I attend this school and will automatically expire after this time.

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can only click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

Only use your own login

My name is :

Agreed by COST Cadets on 19th July 2017

Keeping Safe:
Stop, think, before you Click!

12 Rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's ICT equipment for schoolwork and homework.
2. I will only delete my own files.
3. I will not look at other people's files without their permission.
4. (I will keep my login and password secret.)
5. I will not bring memory/usb sticks into school without permission.
6. I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
7. When using ICT equipment, I will always be polite and sensible.
8. I will not open an attachment, or download a file, unless I have permission.
9. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room.
11. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.
12. I will not take photos or videos of others without permission.

Agreed by COST Cadets on 19th July 2017

Appendix 6

The school has appointed an Online Safety Officer – Tim Filby

The school has appointed an Online Safety Link Governor – Pat Dorling

Appendix 7

Using the Internet safely at home

Whilst many Internet Service Providers offer filtering systems to help you safeguard your child at home, it remains surprisingly easy for children to access inappropriate material including unsuitable texts, pictures and movies. Parents are advised to set the security levels within Internet Explorer with this in mind. Locating the computer in a family area, not a bedroom, will enable you to supervise children as they use the Internet. However, don't deny your child the opportunity to learn from the wide variety of material and games available on the Internet. Instead set some simple rules for keeping them safe and make sure they understand their importance.

Simple rules for keeping your child safe

To keep your child safe they should:

- ask permission before using the Internet
- only use websites you have chosen together or a child friendly search engine
- only email people they know, (why not consider setting up an address book?)
- ask permission before opening an email sent by someone they don't know
- not use Internet chat rooms
- not use their real name when using games on the Internet, (create a nick name)
- never give out a home address, phone or mobile number
- never tell someone they don't know where they go to school
- never arrange to meet someone they have 'met' on the Internet
- only use a webcam with people they know
- tell you immediately if they see anything they are unhappy with.

Using these rules

Go through these rules with your child and pin them up near to the computer. It is also a good idea to regularly check the Internet sites your child is visiting e.g. by clicking on History and Favourites. Please reassure your child that you want to keep them safe rather than take Internet access away from them.

For further information go to:

CEOP: www.ceop.gov.uk
Think U Know: www.thinkuknow.co.uk
Childnet: www.childnet-int.org

Some useful websites

When searching the Internet we recommend you use one of the following child friendly search engines:

Ask Jeeves for kids:
www.askforkids.com

Yahooligans:
www.yahooligans.com

CBBC Search:
www.bbc.co.uk/cbbc/search

Kidsclick:
www.kidsclick.org

Zoo Search:
www.zoo.com

Children, ICT & e-Safety
Information for parents and carers

The purpose of this guide

Children of today are increasingly using Information & Communication Technology (ICT) in schools and in the home. This guide explains:

- How your children are using ICT in school.
- How using ICT in the home can help children to learn.
- How children can use the Internet safely at home.
- Where to access further information.

How your child uses ICT at school

ICT in schools is taught as a subject in its own right and also supports children's learning in other subjects, including English and mathematics. Within ICT lessons children learn to use a wide range of ICT including:

- **Word Processing** to write stories, poems or letters
- **Databases** to record information, e.g. minibeasts
- **Spreadsheets** to create tables, charts and graphs
- **Desktop Publishing** to design posters, leaflets or cards
- **Multimedia Presentation** to present text, pictures and sound
- **Drawing Programs** to create pictures and designs
- **Internet and CD-ROMs** to find information
- **Email** to contact children and teachers in another school
- **Digital Cameras** to record what they have done in class or on a visit
- **Electronic Sensors** to record changes in light, sound and temperature
- **Controllable Robots** to give instructions and make something happen
- **Simulations** to explore real and imaginary situations
- **Website Publishing** to present ideas over the Internet.

How you can help your child at home

ICT is not just about using a computer. It also includes the use of controllable toys, digital cameras and everyday equipment such as a tape recorder or DVD player.

Children can be helped to develop their ICT skills at home by:

- writing a letter to a relative
- sending an email to a friend
- drawing a picture on screen
- using the Internet to research a class topic
- planning a route with a controllable toy
- using interactive games.

A selection of companies offer school software for use at home.

Benefits of using ICT at home

How we know that using ICT at home can help

Many studies have looked at the benefits of having access to a computer and/or the Internet at home. Here are some of the key findings:

- used effectively, ICT can improve children's achievement
- using ICT at home and at school develops skills for life
- children with supportive and involved parents and carers do better at school
- children enjoy using ICT
- using ICT provides access to a wider and more flexible range of learning materials.

How does learning at home using ICT benefit children?

Home use of ICT by children:

- improves their ICT skills
- offers them choice in what they learn and how they learn it
- supports homework and revision
- improves the presentation of their work
- connects learning at school with learning at home
- makes learning more fun.

All this can lead to better performance at school and an improved standard of work. For further information go to:

Parents Centre:
www.parentscentre.gov.uk/usingcomputersandtheinternet.
From the menu choose either **Links by topic** or **Links by age** for details of websites that will support children's learning.

Glossary

Computing (replaces ICT as the National Curriculum subject name)

Online Safety (replaces e-safety)

ICT Information, Communication Technology.

IM Address means Instant Messenger Address, example Yahoo Messenger, WhatsApp etc.

IP address (Internet Protocol address) is a unique address that certain electronic devices use in order to identify and communicate with each other on a computer network.

Portal - A **Web portal** is a single point of access to information which is:

- Linked from various logically related internet based applications and of interest to various type of users
- The WeLearn365.com Portal is a secure Internet space which is available to Warwickshire Schools who have taken part in the We-Learn project.

URL - Uniform Resource Locator, the global address of documents and other resources on the World Wide Web.