Kemble & Siddington C of E Primary Schools
Computing Policy

Purpose of study:

Both schools are committed to providing a high-quality computing education which equips pupils to use computational thinking and creativity to understand and change the world. Computing has deep links with mathematics, science, and design and technology, and provides insights into both natural and artificial systems. The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work, and how to put this knowledge to use through programming. Building on this knowledge and understanding, pupils are equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world.

Aims:

In line with the national curriculum for computing we aim to ensure that all pupils:

- can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation
- 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.

Planning:

Computing is taught through discrete lessons to teach skills and concepts and used in all subject areas to support learning. We have adopted the Wokingham Scheme of Work as the basis for discrete lessons and these are taught on a rolling program. More detailed information can be found on the curriculum map.

Kemble	Autumn	Spring	Summer
Beech (Yr A)	Data retrieving and organising E safety	Communicating E safety	Algorithms and Programs E safety
Beech (Yr B)	Data retrieving and organising E safety	Communicating E safety	Algorithms and Programs E safety
Horse Chestnut (Yr A)	Data retrieving and organising Using the Internet E safety	Databases Presentation E safety	Algorithms and Programs Communicating E safety

Horse Chestnut (Yr B)	Data retrieving and organising Using the Internet E safety	Databases Presentation E safety	Algorithms and Programs Communicating E safety
Chestnut (Yr A)	Data retrieving and organising Using the Internet E safety	Databases Presentation E safety	Algorithms and Programs Communicating E safety
Chestnut (Yr B)	Data retrieving and organising (focus graphics) Using the Internet E safety	Databases (focus spreadsheets) Presentation E safety	Algorithms and Programs Communicating E safety

Siddington	Autumn	Spring	Summer
Robins	Data retrieving and organising E safety	Communicating E safety	Algorithms and Programs E safety
Kingfishers (Yr A)	Data retrieving and organising Using the Internet E safety	Communicating Presentation E safety	Algorithms and Programs Databases E safety
Kingfishers (Yr B)	Data retrieving and organising Using the Internet E safety	Communicating Presentation E safety	Algorithms and Programs Databases E safety
Owls (Yr A)	Data retrieving and organising Using the Internet E safety	Databases Presentation E safety	Algorithms and Programs Communicating E safety
Owls (Yr B)	Data retrieving and organising Using the Internet E safety	Databases Presentation E safety	Algorithms and Programs Communicating E safety
Owls (Yr C)	Data retrieving and organising Using the Internet E safety	Databases Presentation E safety	Algorithms and Programs Communicating E safety

Sessions are then outlined, using the school Medium Term planning grids, recording session aims, key skills and outcomes.

Links to other subjects:

Computing links to other subjects. Links are made clear within the Medium Term Planning Document and Topic Planning Map where key skills are identified.

Assessment for Learning:

Assessment data is collected 3 times a year to monitor attainment and progress in the two schools. A tracking spreadsheet, linked to the Wokingham Scheme of Work is available for teachers to build an on-going record.

Teachers assess before, during and after teaching to inform planning. Lessons can then be adapted for individual or groups of children's needs.

Subject leadership:

The coordination and planning of the computing curriculum is the responsibility of the subject leader, who also:

- supports colleagues in their teaching, by keeping informed about current developments and by providing a strategic lead and direction for this subject;
- gives the head teacher & governors an annual summary report in which s/he evaluates the strengths and weaknesses in computing and indicates areas for further improvement;
- uses specially allocated regular management time to review evidence of the children's work, and to observe both computing lessons and activities of cross curricular skill application across the school.

Resources:

Both schools have a combination of Windows based laptops and iPads for use across the school.
These are updated on a rolling program as the need arises.
Suggested Resources to support learning include:

The Wokingham Scheme of Work for Computing
Somerset Scratch resources
(https://slp.somerset.org.uk/sites/edtech/SitePages/Primary%20Computing/Scratch.aspx)
Barefoot Computing (http://barefootcas.org.uk/)
Kodable (https://www.kodable.com/resources)
Computing at School (http://community.computingatschool.org.uk/resources)
BBC Computing (http://www.bbc.co.uk/schools/0/computing/28972462)
Simon Haughton's Website (http://www.simonhaughton.co.uk/ict-lessons/)

Kemble & Siddington C of E Primary Schools
E-safety and Acceptable use of the Internet Policy

Rationale

The internet has become an important aspect of everyday life and children need to be able to use it safely and responsibly. At Kemble and Siddington Primary Schools, we believe that the internet offers a valuable resource for teachers and children, as well as providing new ways to communicate with others worldwide. At the same time our schools recognise that there are many risks related to using the internet and this policy sets out the measures to be taken to minimise them.

1. Leadership and Management

The school e-safety policy features as part of the policy review cycle and it is related to other policies including those for child protection, behaviour, PSHCE and anti-bullying. This policy will be reviewed on annual basis and will be ratified by the staff and the governors.

1.2 How will Internet access be authorised?

We believe that internet access for pupils is an entitlement on the basis of educational need and is an essential resource for staff. Parents of reception children complete the Responsible Acceptable Use agreement form and pupils take responsibility for signing this form from Yr 3. The South West Grid for Learning (SWGfL) proactively monitors internet usage for illegal (attempted access of child abuse and incitement for racial hatred) websites and will notify the local police and Gloucestershire LA in these instances.

In school, we will keep a record of all staff and pupils who are granted internet access. Children will only use the internet under supervision or instruction by adults in KS1. Any independent searches undertaken by pupils in KS2 will be done so in a supervised environment.

1.3 How will filtering be managed?

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access is tailored so that it is appropriate for all members of the school community from the youngest pupil to staff. As we are part of the SWGFL no members of staff have unfiltered access to the internet.

We work closely in partnership with parents, Gloucestershire LA, DFE and the SWGfL to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider (SWGfL). This should also be logged by staff into our Internet Incident Log. Website logs will be regularly sampled and monitored. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that we believe to be illegal will be referred to the Internet Watch.

1.4 How will the risks be assessed?

As the quantity and breadth of the information available through the internet continues to grow it is not possible to guard against every undesirable situation. However, the school will address the issue that it is difficult to remove completely; the risk that pupils might access unsuitable materials via the school system.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. Kemble and Siddington Primary Schools 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 Gloucestershire LA can accept liability for the material accessed, or any consequences of internet access. It is important to remember that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

We will regularly review methods to identify, assess and minimise risks and the head teacher will ensure that the policy is implemented and compliance with the policy is monitored.

Teaching and Learning

2.1 Why is internet use important?

The internet is an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning along with the skills to use it safely. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the school's management information and business administration systems. The internet is an essential part of everyday life for education, business and social interaction. Our school has a duty to provide students with quality internet access as part of their learning experience. It is also important to remember that pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.

2.2 How will internet use enhance learning?

Using the Internet in education has many benefits including:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;

- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments,
- Educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

<u>2.3 How will pupils learn to evaluate internet content?</u>

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. Ideally, inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. In school, we educate pupils about what to do if they experience material that they find distasteful, uncomfortable or threatening.

E-safety skills are integral to the National Curriculum and are taught every term.
Through e-safety education, pupils will:

- Be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy;
- Use age-appropriate tools to research Internet content;
- Be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Use social networking responsibly and respectfully.

3. Communication and Content

<u>3.1 The School Website</u>

The point of contact on the website is the school address, school email and telephone number. Staff or pupils' home information will not be published. Website photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the website. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or Blogs. Where audio and video are included (e.g. podcasts and video blogging) the nature of the items uploaded will only be included with parental permission. The website complies with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.2 Learning Platforms

Senior Leadership Team (SLT) and staff will regularly monitor the usage of any learning platforms (LP) by pupils and staff in all areas, in particular message and communication tools and publishing facilities. All pupils/staff will be advised about acceptable conduct and use when using learning platforms. Only members of the current pupil, parent/carers and staff community will have access to the LP. All users will be mindful of copyright issues and will only upload appropriate content onto the LP. When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

3.3 Managing e-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures. Currently we do not give children personal use of email identities such as john.smith@kemble.gloucs.sch.uk as revealing this information could potentially expose a child to identification by unsuitable people. Pupils should not use personal email addresses in school. However, if a lesson requires the children to use email, it should be strictly monitored by the teacher and using an approved class e-mail account on the school system.

Pupils must immediately tell a responsible adult if they receive offensive e-mail. Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.

All staff will use official school provided email accounts and e-mail sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper. When sending email, children should be referred to by their initials. Any sensitive documents sent by email should by password protected.

3.4 On-line communications, social networking and social media

On-line communications, social networking and social media services are filtered in school by the SWGfL but are likely to be accessible from home and on mobile devices.

Through regular training, all staff are made aware of the potential risks of using social networking sites or publishing either professionally with students or personally. Staff should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils are encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. We have a key role in teaching young people about the importance of keeping personal information safe.

- Pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils must not reveal personal details of themselves or others in online communication, or arrange to meet anyone.

- Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the senior leadership team before using social media tools in the classroom.
- Staff/class official blogs or wikis are password protected and run with approval from the SLT.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. These are moderated by the school where possible.
- Pupils are advised on security and privacy online and are encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils are encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.

3.5 Mobile phones and personal devices

Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, social networking capabilities, instant messaging, cameras and internet accesses all common features.

Children are not allowed to bring mobile devices into school unless the headteacher agrees that it is an 'exceptional circumstance'. In these cases, the class teacher should look after the mobile phone for the child. School staff may confiscate a mobile phone or device if its use has not been sanctioned by the headteacher. Any electronic devices that are brought in to school are the responsibility of the user. Our school accepts no responsibility for the loss, theft or damage of such items.

Except in exceptional circumstances, Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Where practical, staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose. If personal devices are used then photos should be removed as soon as practicable.

3.6 Video Conferencing

Videoconferencing (Skype, Microsoft Lync face time etc) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education.

When doing this, staff must refer to the internet consent agreements prior to children taking part in videoconferences. All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer. Pupils will ask permission from a teacher before making or answering a videoconference call. Videoconferencing will be supervised appropriately for the pupils' age and ability.

3.7 Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, internet access, collaboration and multimedia tools. Access of new technologies will be denied until they have been deemed appropriate by the SLT. They will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.8 Cyberbullying

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyberbullying can be defined as:

'The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone' DCSF 2007.

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policies on anti-bullying and behaviour.
- Incidents or allegations of cyberbullying will be investigated following the procedures outlined the anti-bullying policy.
- Anyone in our school community who is affected by cyberbullying will be supported in accordance with the anti-bullying policy.
- All incidents of cyberbullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This includes examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Pupils, staff and parents/carers are required to work with the school to support the approach to cyberbullying and the school's e-safety ethos.

3.9 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

All data from which people can be identified is protected. To access the school network, staff must use their unique passwords and usernames. Staff must password protect sensitive documents when sending them by email. Children's names will not be referred to directly within the content of emails. All Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

3.10 Staff use of Social Networking

The school is aware that an increasing number of adults and children are using social networking sites such as FaceBook snapchat and Instagram.

The use of social networking provides us with many benefits, from improved communication skills and a greater understanding of technology to a more open worldview. However, we feel that certain behaviour on such websites can potentially have a detrimental effect on the image of the school, our ability to safeguard our pupils and on the integrity of our staff.

Through the following expectations, we hope to: protect staff from allegations and misinterpretations which can arise from the use of social networking sites; make explicit the standards of behaviour and/or codes of practice linked to social networking for educational; personal or recreational use; and to support our stance on safeguarding of children as outlined in our Child Protection policy.

Expectations

- School representatives must not be involved in communication with current pupils via social networking, where the staff member has legitimate links (for example family) then the headteacher should be informed.
- School representatives must not use carry out actions that would breach school codes of conduct or policies relating to staff.
- That all school representatives have the strictest form of privacy on any personal online content, meaning that they choose who can see their content.
- Social Networking should not be used to publicly discuss matters (positive or negative) related to school and consider carefully the subjects that they discuss
- School representatives should avoid information or conversations that could compromise their professional integrity.

- Any embarrassing wall posts should be avoided, and representatives should discuss whether they are happy for images to be posted

4 Implementation

4.1 Introducing the Policy to Pupils

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of our e-safety teaching and awareness-raising it is important to discuss the key features with pupils as appropriate for their age. Pupils may need to be reminded of the school rules at the point of Internet use.

- All users will be informed that network and internet use will be monitored.
- An e–safety training programme is taught across the school.
- Pupil instruction regarding responsible and safe use will precede all internet access.
- E–safety will be included in the PSHCE curriculum and will be taught throughout the school as part of ICT. Both safe school and home use will be covered.
- E-safety rules or copies of the pupils Acceptable Internet Use Policy are posted in all rooms with internet access.
- Safe and responsible use of the Internet and technology is reinforced across the curriculum and subject areas.

4.2 Consulting with Staff

It is important that all our staff feel confident to use new technologies in teaching and our school e–safety policy will only be effective if all staff subscribe to its values and methods. The staff are involved in the policy review process and are given opportunities to discuss the issues and develop appropriate teaching strategies.

All staff must understand that the rules for information systems misuse for Gloucestershire County Council employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with the ICT subject leader to avoid any possible misunderstanding.

- The e–Safety Policy will be formally provided to and discussed with all members of staff. The staff will be involved in its review.
- Staff should be aware that internet traffic is monitored and reported by the SWGfL and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff should be aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

4.3 Parents and E-Safety

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.

- The school website is used to promote a number of e-safety resource websites that parents can use at home with their children.
- Parents are given the opportunity to take part in regular parent e-safety learning sessions run by the SWGFL. Parents will also be given the opportunity to learn alongside their children in 'parent learning sessions'.
- Through our school newsletter and website, regular information is provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet are available to parents.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).
- All parents are aware of who the ICT subject leader is and will receive support information as and when available, e.g. Know It All for Parents.

4.4. How will complaints be handled?

Parents and teachers must know how and where to report incidents. Prompt action is required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to our behaviour policy. All record of the incident are kept, e.g. e-mails saved or printed, text messages saved etc. All complaints of a child protection nature will be dealt with in accordance with the LA Child Protection procedures.

- Responsibility for handling incidents will be the responsibility of E-Safety Coordinator and SLT.

Any complaint about staff misuse must be referred to the headteacher.

Appendix 1

E-SAFETY – School / home information & help sheet

All parents need to be aware of the many dangers that new technologies can present. Please use the two following websites to learn about the dangers and how you can keep your children safe.

Website 1 – Thinkyouknow

Parent section then tab to Advice if your children are in primary education. There are lots of things to look at – but recommended:

- ❖ Growing up online (what is my child doing?)
- ❖ Conversation Starters (how do I talk to my child about what they are doing?)
- ❖ Risks my child might face (what risks might they be facing?)
- ❖ Tools to protect my child (what tools are there to help us?)

Tips from this website:

Talk to your child about what they're up to online. Be a part of their online life; involve the whole family and show an interest. Find out what sites they visit and what they love about them, if they know you understand they are more likely to come to you if they have any problems.

Watch Thinkuknow films and cartoons with your child. The **Thinkuknow site** has films, games and advice for children from five all the way to 16.

Encourage your child to go online and explore! There is a wealth of age-appropriate sites online for your children. Encourage them to use sites which are fun, educational and that will help them to develop online skills.

Keep up-to-date with your child's development online. Children grow up fast and they will be growing in confidence and learning new skills daily. It's important that as your child learns more, so do you.

Set boundaries in the online world just as you would in the real world. Think about what they might see, what they share, who they talk to and how long they spend online. It is important to discuss boundaries at a young age to develop the tools and skills children need to enjoy their time online.

Keep all equipment that connects to the internet in a family space. For children of this age, it is important to keep internet use in family areas so you can see the sites your child is using and be there for them if they stumble across something they don't want to see.

Know what connects to the internet and how. Nowadays even the TV connects to the internet. Make sure you're aware of which devices that your child uses connect to the internet, such as their phone or games console. Also, find out how they are accessing the internet – is it your connection, or a neighbour's wifi? This will affect whether the safety setting you set are being applied.

Use parental controls on devices that link to the internet, such as the TV, laptops, computers, games consoles and mobile phones. Parental controls are not just about locking and blocking, they are a tool to help you set appropriate boundaries as your child grows and develops. They are not the answer to your child's online safety, but they are a good start and they are not as difficult to install as you might think. Service providers are working hard to make them simple, effective and user friendly. **Find your service provider and learn how to set your controls**

Website 2 – Common Sense Media – this website (although USA based) is very good for parent tips – with excellent video clips that you can watch on your own or with your children and then chat together.

Recommended – Use the Parent concerns tab, the list then includes:

- ❖ Screen time
- ❖ Cyberbullying, Haters & Trolls
- ❖ Privacy & Internet Safety
- ❖ Facebook, Instagram & Social
- ❖ Cell Phone Parenting
- ❖ Violence in the Media
- ❖ Sex, Gender & Body Image
- ❖ Alcohol, Drugs & Smoking
- ❖ Marketing to Kids
- ❖ Learning with Technologies
- ❖ Reading
- ❖ Special Needs and Learning Difficulties

Example – Cyberbulling, Haters & Trolls if clicked on presents 22 FAQs, 7 articles and 8 videos to watch.

Privacy & Internet safety has 25 FAQs, 5 articles and 10 videos – a good one is 'How do I protect my kid's privacy on line?'

Browse and look at the areas – not all at once – there is a lot to take in. The whole website is very informative.

AND FINALLY….

Remember if you start chatting and being involved with their online friends and forums now it will be easier to be involved when they are teenagers. I was told that you would not let anyone play and chat to your child face to face, so use the same rules online.

Grooming is rare, unfortunately cyberbullying is not – both need to be talked to with your child just as you would teach them about road safety or stranger danger.

Your children will be taught all aspects of online safety (at age appropriate times) in their school curriculum, but it is very important that we both help keep your children safe and work together.

Appendix 2

Kemble and Siddington C of E Primary Schools

Responsible Internet Use

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

- I will always ask before using computers in school.
- I will always ask an adult in school before using the internet.
- I will use only my personal/class login and password, which is secret.
- I will only open my own files and ask a teacher before deleting anything.
- I understand that social networking should only be used outside school with my parents' permission.
- I must ask an adult before using any external hardware (memory sticks, CDs etc) .
- I will only e-mail and open attachments that my teacher has approved.
- The messages I send will be polite and sensible.
- I understand the importance of keeping my personal information safe.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers for specific amount of time, decided by my teacher. My parents will be told if this happens.
- I understand that, for my safety, the school is allowed to monitor my internet activity, including emails and the websites that I look at.
- I know that the South West Grid for Learning (SWGfL) monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.

Kemble and Siddington C of E Primary Schools

Responsible Internet Use

Please complete, sign and return to the school

Pupil: ***Class:***

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

Signed: ***Date:***

Parent's Consent for Internet Access

I have read and understood the school rules for responsible internet use and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions using filtering provided by SWGFL to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: ***Date:***

Please print name:

Parent's Consent for Web Publication of Work and Photographs and Use of Digital Communications

I agree that, if selected, my son/daughter's work may be published on the school website , class and school Blogs. I also agree that images, sound files and video that include my son/daughter may be published on the website, Blogs and local newspapers subject to the school rules that this content will not clearly identify individuals and that full names will not be used. I understand that children may take part in online digital communication activities such as Skype or similar activities as part of their learning.

Signed: ***Date:***

Appendix 3

Kemble and Siddington C of E Primary Schools
Laptop Policy for School Staff

1. The laptop remains the property of the school.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only school staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to the school. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the headteacher).
4. Whenever possible, the laptop must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
5. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.
6. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
7. Any software loaded must not affect the integrity of the school network.
8. If any removable media is used then it must be checked to ensure it is free from any viruses.
9. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up-to-date.
10. Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated.
11. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
12. Students can only use the laptop with permission and close supervision.
13. If any fault occurs with the laptop, it should be referred immediately to the network manager.
14. When being transported, the carrying case supplied must be used at all times.
15. The laptop would be covered by normal household insurance. If not it should be kept in school and locked up overnight.

Policy for responsible e-mail, network and internet use

1. I will use all ICT equipment issued to me in an appropriate way. I will not:
   - Access offensive website or download offensive material.
   - Make excessive personal use of the Internet or e-mail.
   - Copy information from the internet that is copyright or without the owner's permission.
   - Place inappropriate material onto the Internet.
   - Will not send e-mails that are offensive or otherwise inappropriate.
   - Disregarded my responsibilities for security and confidentiality.
   - Download files that will adversely affect the security of the laptop and school network.
   - Access the files of others or attempt to alter the computer settings.
   - Use social medial on school laptops.
   - Update web pages etc. or use pictures or text that can identify the school, without the permission of the headteacher.
   - Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school.

2. I will only access the system with my own name and registered password, which I will keep secret.
3. I will inform the ICT Subject Leader as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working. ·
5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the headteacher and register the passwords with the headteacher.
7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
8. I will always adhere to the school ICT, Social Networking and E-safety policies.
9. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the ICT subject leader.
10. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
11. I will report immediately to the headteacher any unpleasant material or messages sent to me.
12. I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material.
13. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
14. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity.
15. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
16. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.
17. If I email any sensitive pupil information or data, I will password protect the document and then send a separate email with the password if needs be.

Name..

Signature: ....

Date: ....