Sherborne St John Church of England Primary School

Policy for E-Safety

1. Introduction

Sherborne St John Church of England Primary School recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process. This e-safety policy should be read in conjunction with other relevant school policies e.g. safeguarding procedures, Anti Bullying and Child Protection.

2. Creation, Monitoring and Review

The school e-Safety Policy has been written by the Computing Manager and passed to the Teachers and Governors to be reviewed and accepted as a policy.

The impact of the policy will be monitored regularly with a full review being carried out every 2 years. The policy will also be reconsidered where concerns are raised by members of the school staff, students or Governors or where an e-safety incident has been recorded.

3. Policy Scope

The policy applies to all users of the school community who have access to the school IT systems, both on the premises and remotely. Any user of school IT systems must adhere to and sign a hard copy of the Acceptable use Policy/AUP (see appendix 1). The e-Safety Policy applies to all use of the internet and electronic communication devices such as email, internet explorer, mobile phones, games consoles, iPads, social networking sites and instant messaging.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

4. Roles and Responsibilities

All members of the school should know who is responsible for e-safety. It should be clear to whom they can report concerns or gain further information.

There are clear lines of responsibility for e-safety within the school. For children the first point of contact should be their teacher or Learning Support Partner. All staff are responsible for ensuring the safety of students and should report any concerns immediately to the e-safety co-ordinator/ Computing Manager. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Child Protection Officer may be asked to intervene with appropriate additional support from external agencies.

E-safety officer/ Computing Manager:
Our e-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The e-safety coordinator at present is **Sarah Biles**. It is the responsibility of the e-safety coordinator to:

- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provide training and advice for staff
- liaise with the Local Authority for guidance
- liaise with school ICT technical staff (Techs 4 Education)
- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meet with e-safety governor to discuss current issue and review incident logs
- attend relevant meetings and committees of Governing Body
- reports regularly to the Headteacher and Deputy Headteacher
- receive appropriate training and support to fulfil their role effectively
- have responsibility for reporting inappropriate content to ICT technical staff (Techs 4 Education) to contact Hampshire who would then block internet sites in the school's filtering system

- Maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices

Responsibilities: governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety governor which involves:

- regular meetings with the E-Safety Co-ordinator with an agenda based on:

• monitoring of e-safety incident logs

• monitoring of filtering change control logs

• monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices

• reporting to relevant Governors committee / meeting

Responsibilities: Head Teacher

- The head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator

- The head teacher and another member of the senior management team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see Figure 1)

Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

- they have read, understood and signed the school's Acceptable Use Policy for staff (see appendix 1) and must actively promote this through embedded good practice. This policy has been agreed by unions and verified by the legal team in Hampshire County Council

- they report any suspected misuse or problem to the E-Safety Co-ordinator

- digital communications with students (email / learning platform/ voice) should be on a professional level and only carried out using official school systems. Contact with students through social networking sites and instant messaging is prohibited

- e-safety issues are embedded in the curriculum and other school activities

Responsibilities: ICT Technical Staff (Techs 4 Education)
The ICT Technical staff are responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are reported to the Computing coordinator or Headteacher so that appropriate action may be taken

5. Security

The school will do all that it can to make sure the school network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of school systems and information.

Filtering
At present our school network is filtered directly from Hampshire County Council. If an inappropriate image or website is not blocked staff must report this straight away to the E-Safety officer who will then contact Hampshire County Council to see that it becomes filtered.

6. Behaviour

Online communication can take many forms, whether it is by email, text, video conferencing or instant chat. It is essential that all students and staff are aware of existing school policies that refer to acceptable behaviours when communicating online.

Sherborne St John Church of England Primary School will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy.

The school will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the appropriate student and staff disciplinary policies.

Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police.

7. Acceptable Use Policies (AUP)

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable use policies are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers (including permissions to use pupil images / work and to use ICT systems)

Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents.

For children in EYFS and KS1 parents may sign on behalf of their children.

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the schools ICT resources (including the internet) and permission to publish their work.

Induction policies for all members of the school community include this guidance.

8. Illegal or inappropriate activities

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

• **child sexual abuse images (illegal - The Protection of Children Act 1978)**

• **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**

• **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**

• **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**

• pornography
• promotion of any kind of discrimination

• promotion of racial or religious hatred

• threatening behaviour, including promotion of physical violence or mental harm

• any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable:
• Using school systems to run a private business

• Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Hampshire County Council and / or the school

• Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions

• Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)

• Creating or propagating computer viruses or other harmful files

• Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet

• On-line gambling and non-educational gaming

• Use of personal social networking sites / profiles for non-educational purposes

9. Sanctions

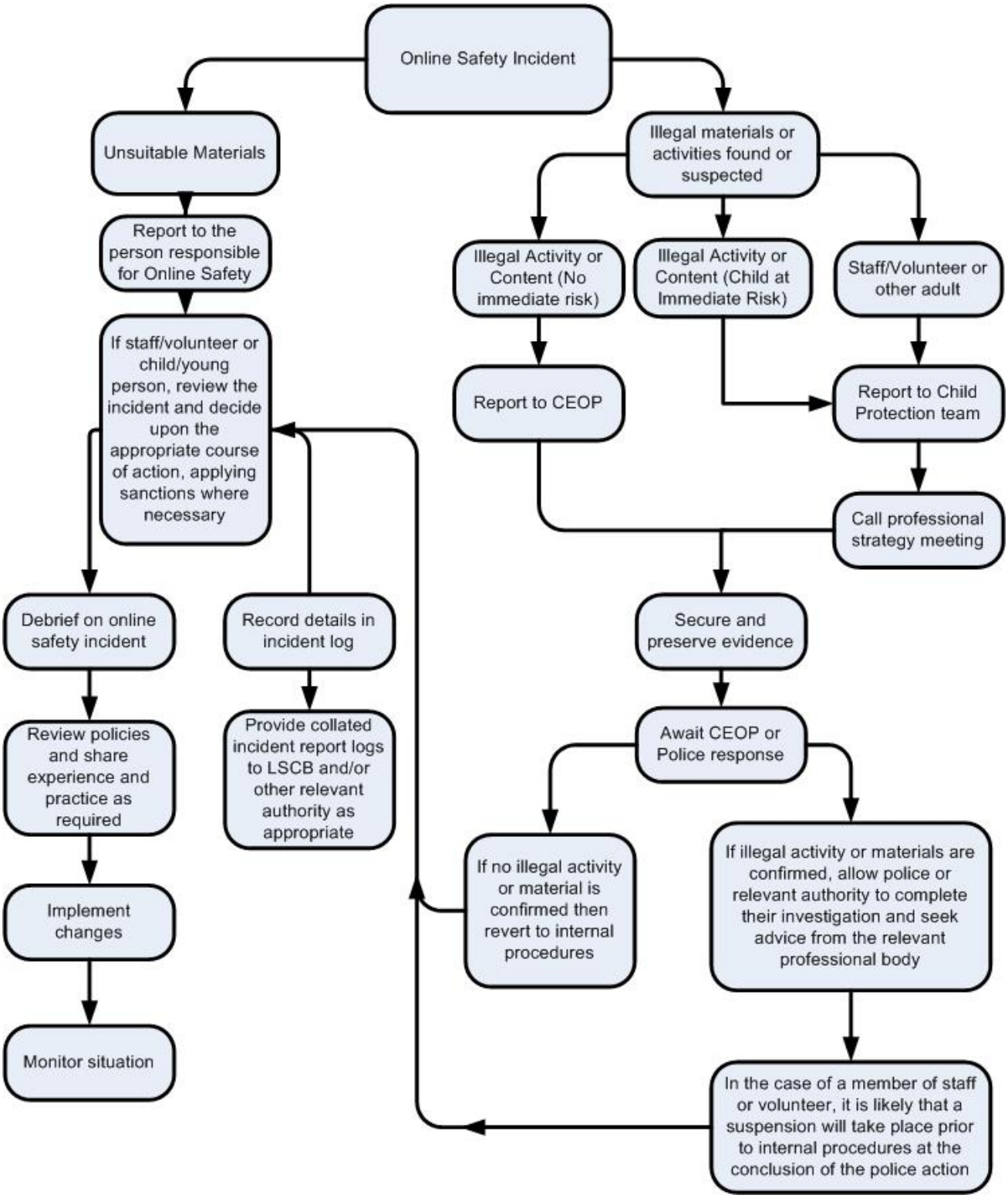
If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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.

10. Procedures

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 in **Figure 1** are the responses that will be made to any apparent or actual incidents of misuse.

Figure 1


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

11. Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:

o Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances

o Members of staff are free to use these devices in school, outside teaching time and not in front of children.

- Pupils are permitted to bring in hand held devices and mobile phones however they must be handed into the office or their class teacher at the beginning of the day.

12. Email

Access to email is provided for all users in school via the intranet page accessible via the web browser (internet Explorer) from their desktop.

These official school email services may be regarded as safe and secure and are monitored.

- Staff use only the school email services to communicate with others when in school, or on school systems (eg by remote access). All communications relating to school business should be via school email addresses rather than personal email addresses

- Users need to be aware that email communications may be monitored

- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email

- Staff may only access personal email accounts on school systems during their breaks (these may be blocked by filtering)

- Users must immediately report, to the e-safety coordinator – 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.

13. Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites

- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section for guidance on publication of photographs

14. Use of web-based publication tools

Our school uses the public facing website, www.ssj-school.co.uk for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content. Our school also uses the twitter feed @SherborneSJPE which is for sharing good practise in PE and activities carried out in and out of school. Children's names are never used on twitter and parental permission if obtained. There is also a live feed from our website.

- Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils)

- Only pupil's first names are used on the website, and only then when necessary

- Detailed calendars are not published on the school website

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:

pupils' full names will not be used anywhere on a website or blog, and never in association with photographs. Permission from parents or carers will be obtained before photographs of pupils are published on the school website.

- Any photographs taken in relation to the twitter account will be deleted from personal phones in a timely manner.

15. E-safety education

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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of Computing, PSHE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school

- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Caf at KS2)

- Learning opportunities for e-safety are built into the school curriculum for Computing

- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises

- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school

- 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit

We will also offer e-safety information to parents through specific information evenings, the school website, newsletters and meetings with individual parents.

16. Social Media

As a school we recognise that social media and networking are playing an increasing role within everyday life and that many staff, governors and parents are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff, governors and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

As a school access to social networking sites is blocked, via Hampshire County Council, on all school computers.

Staff and governors should:

- ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- not accept current or ex-pupils as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members live and have friends within the local community and ask that these members of staff take extra care when posting online
- ensure that their communication maintains their professionalism at all times
- be aware that electronic texts can be misconstrued so should endeavour to minimise the possibility of this happening
- not use these media to discuss confidential information or to discuss specific children
- check with the Computing subject leader or ICT technician if they need advice on monitoring their online persona and checking their security settings

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that some are signed up with, or without, parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will ensure that parents are aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying occur.

As a school we may introduce blogging with our new website that is being launched in the near future. If this is the case we shall amend this policy to provide guidelines in how this shall be used.

17. Cyber Bullying

Cyber-bullying can leave children and young people feeling scared, upset and very vulnerable, particularly as they can be victimised in their own home.
There are a number of different methods of cyber-bullying, but the main ones are:

- Sending emails and other messages to individuals or groups that are threatening, upsetting or offensive and may include racism, sexism, or homophobic content

- Sending emails and other messages to friends of the victim to try to make them become part of the bullying

- Profiles can be set up on social networking sites to make fun of a child or young person, and if others contribute to the profiles they may become part of the bullying

- Mobile phones can be used for sending humiliating and abusive phone calls, texts, photos or video messages, e.g. some children or young people have shared inappropriate images of themselves and others, as well as videos of physical attacks on others

- Children and young people involved in interactive gaming can chat online with other players, and cyber-bullies can abuse other players, use threats, lock victims out of games, spread false rumours

- Some young people are able to send viruses or hacking programs that can destroy the victim's computer or delete personal information from their hard drive

- Many victims of cyber-bullying have seen their personal information such as photos, emails or blogs posted where others could see them without their permission

18. Information literacy

Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:

- Checking the likely validity of the URL (web address)

- Cross checking references (can they find the same information on other sites)

- Checking the pedigree of the compilers / owners of the website

- See lesson 5 of the Cyber Caf Think U Know materials below

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils are taught how to make best use of internet search engines to arrive at the information they require

- We use the resources on CEOP's Think U Know site as a basis for our e-safety education

19. Staff training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly
- It is expected that some staff will identify e-safety as a training need within the performance management process
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority, the HSCB and others
- All teaching staff have been involved in the creation of this e-safety policy and are therefore aware of its content
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis

19. Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line 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.

The school will therefore seek to provide information and awareness to parents and carers through:

 Letters, newsletters, web site

 E-safety evening for parents as well as parent consultation evenings

 Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others

Professionals

CEOP (Child Exploitation and Online Protection) Safety Centre http://www.ceop.police.uk/safety-centre

Childnet International	http://www.childnet.com
Know IT All	http://www.childnet-int.org/kia/
Professionals Online Safety Helpline (UKSIC)	Email helpline@saferinternet.org.uk or telephone 0844 381 4772
SWGfL Staying-Safe (South West Grid for Learning)	http://www.swgfl.org.uk/Staying-Safe
Think U Know (CEOP)	http://www.thinkuknow.co.uk/
UK Safer Internet Centre (UKSIC)	http://www.saferinternet.org.uk/

Children, Young People & Families

A Parent's Guide to Technology (UKSIC)	http://www.saferinternet.org.uk/advice-and-resources/a-parents-guide
onnect Safely	http://www.connectsafely.org
Digizen	http://www.digizen.org
KidSmart	http://www.kidsmart.org.uk/
Get Safe Online	http://www.getsafeonline.org/
Know IT All	http://www.childnet-int.org/kia/parents/
Think U Know	http://www.thinkuknow.co.uk/

This policy was approved by the Governors on 25.11.15

Reviewed Autumn 2017, 2018

Review Autumn 2019

Appendix 1

ICT Acceptable Use Agreement

for Staff (and Volunteers)

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's E-Safety Co-ordinator for further information and clarification.

▫ I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

▫ I understand that I must not use the school ICT system to access inappropriate content

▫ I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

▫ I understand that school information systems **and hardware** may not be used for private purposes without specific permission from the head teacher.

▫ I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

▫ I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.

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

▫ I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. It must only be kept on encrypted removable storage devices.

▫ I will respect copyright and intellectual property rights.

▫ I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

▫ I will report any incidents of concern regarding children's safety to the schools e-Safety Coordinator, the Designated Child Protection Liaison Officer or Head teacher.

▫ I will ensure that electronic communications with pupils including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

▫ I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: …… Capitals: …… Date: ……

Accepted for school: …… Capitals: ……

Appendix 2

ICT Acceptable Use Agreement for Pupils

E-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed **Date**

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rules.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

In the absence of any negligence, I understand that the school and HCC cannot be held responsible for the content of materials accessed through the internet. I agree that the school and HCC are not liable for any damages arising from use of the internet facilities.

Signed **Date**

Please print name:

E-Safety Rules

Key Stage 1

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 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. • We can send and open emails together. • We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click
These rules help us to stay safe on the Internet: • We ask permission before using the Internet. • We only use websites that an adult has chosen. • We tell an adult if we see anything we are uncomfortable with. • We immediately close any web page we are not sure about. • We only email people an adult has approved. • We send emails that are polite and friendly. • We never give out personal information or passwords. • We never arrange to meet anyone we don't know. • We do not open emails sent by anyone we don't know. • We do not use Internet chat rooms.