Haddenham St Mary's CE School

E-SAFETY POLICY

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- HSM school has appointed an e-Safety Coordinator.
- HSM has Designated Child Protection Officers
- Our e-Safety Policy has been written in conjunction with Bucks e-Safety Policy and government guidance.

Teaching and learning

Benefits of using the internet in education include:

- Access to worldwide educational resources
- Access to learning and wherever and whenever convenient
- Educational and cultural exchanges between pupils world-wide
- Professional development for staff through access to national developments, educational materials and effective classroom 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
- Exchange of curriculum and administration data with Bucks County Council.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils to enhance and extend education. Access levels will be reviewed to reflect the curriculum requirements and age of pupils
- Pupils will be taught what Internet use is acceptable and what is not through our units on keeping safe
- The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work
- Pupils will be shown how to publish and present information to a wider audience

Pupils will be taught how to evaluate Internet content

- The evaluation of online materials is part of teaching/learning in every subject
- Pupils will be taught the importance of cross-checking information before accepting its accuracy through teacher led activities
- Pupils and staff will be taught how to report unpleasant internet content (i.e. report it to the Head teacher who will then contact the network support team to have the site filtered)

Managing Internet Access

Published content and the school web site

- Staff or pupil personal contact information will not be published
- The contact details on the website are the school address, email and telephone number
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing pupil's images and work

- All parents or carers sign forms on entry giving or with-holding permission for photographs to be published on the school web site or in the media
- Pupils' full names will not be used anywhere on a school web site or other online space, particularly in association with photographs
- Pupil image file names will not refer to the pupil by name
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing

- **HSM strongly discourages infant school aged pupils to access social networking sites**
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils
- Staff should not access social networking sites in school time on school computers or iPads
- Staff should not run social network spaces for pupil use out of the school network
- Staff will adhere to the rule that any new friend request from a child or parent in their school must NOT be accepted. Equally no staff should request a new friendship with a current pupil or parent.
- Staff should not post any comments on social networking sites that might be considered derogatory to the school
- Newsgroups will be blocked unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind, which may identify them, their friends or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of family/friends, specific interests and clubs
- Pupils will be advised not to place personal photos on any social network space
- Advice will be given regarding background detail in a photograph which could identify the pupil or his/her location
- Pupils will be advised to use nicknames and avatars if using social networking sites
- Pupils and staff are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Managing filtering

- The school will work with the Bucks County Council, and the BITES team to ensure systems to protect pupils are reviewed and improved
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher
- Staff will ensure that annual checks are made to ensure that the Bucks County Council and the BITES team filtering methods selected are appropriate, effective and reasonable
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF (internet watch foundation) or CEOP

Managing videoconferencing & webcam use (if available)

The equipment and network

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer
- School videoconferencing equipment should not be taken off school premises without permission
- Videoconferencing contact information should not be put on the schools website.
- Pupils should ask permission from the teacher before making or answering a videoconference call
- Parents and carers should agree for their children to take part in videoconferences.
- When recording a videoconference lesson, written permission should be given by all sites and participants

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications
- Mobile phones will not be used during lessons or around pupils. The sending of abusive or inappropriate messages or files is forbidden
- The use by pupils of cameras in mobile phones is not allowed on school premises. **No pupils should have a mobile phone in school**
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read and sign the “Staff Code of Conduct’’ before using any school ICT resource

- Access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials
- Parents will be asked to sign and return a consent form when pupils enter the school – The Netsmart Pupil Code of Conduct
- Any person not directly employed by the school will be reminded of appropriate use of technology with regard to safeguarding as required

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer or iPad connected to the school network. Neither the school nor Buckinghamshire County Council can accept liability for any material accessed, or any consequences resulting from of internet use.

E-safety complaints

- Complaints of internet misuse will be dealt with by the Headteacher or Chair of Governors. Staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the internet
- All e-safety complaints and incidents will be recorded by the school – including any actions taken

Community use of the Internet

- The school will be sensitive to internet related issues experienced by pupils out of school, eg social networking sites, and offer appropriate advice

How will cyberbullying be managed?

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Should an instance occur, the following will take place:

- Support for anyone affected by cyberbullying
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying possible witnesses, and contacting the service provider if necessary

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive
- Service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.

- Parent/carer will be informed

Communications Policy

Introducing the e-safety policy to pupils

- E-Safety rules are discussed with pupils frequently as part of the ICT curriculum and are displayed around school
- Pupils will be informed that network and internet use will be monitored and appropriately followed up
- E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum covering both safe school and home use
- Pupils will be familiarised with the Pupils' NetSmart Code of Practice

Staff and the e-Safety policy

- All staff and governors will be given the School e-Safety Policy and its importance explained
- To protect all staff and pupils, the school will implement acceptable use policies
- Staff must be informed that network and internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Staff will always use a child friendly safe search engine when accessing the web with pupils
- All staff will sign the Staff NetSmart Code of Practice document.

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school web site
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school
- Information and guidance for parents on e-safety will be made available to parents in a variety of formats

The public sector equality duty of the Equality Act 2010 has been considered in the writing of this policy. A Discrimination Impact Assessment concludes that through this policy Haddenham St Mary's School seeks to:

- Eliminate discrimination, harassment and victimisation and other conduct prohibited by the Act
- Advance equality of opportunity between people who share a protected characteristic and those who do not
- Foster good relations between people who share a protected characteristic and those who do not
- Protect Characteristics: age, disability, gender, gender identity, race, religion or belief, and sexual orientation.

Appendix 1: Useful resources for teachers

Please refer to the DfCSF e-safety policy guidance for further information.

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Becta
http://schools.becta.org.uk/index.php?section=is

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

Bucks e-Safety Policy and Guidance, Posters etc

Kidsmart
www.kidsmart.org.uk

Bucks Policy – e-Safety

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 2: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

Appendix 3: E-Safety Audit – Primary

This self-audit should be completed annually by the staff member responsible for the e-safety policy.

Date audit completed:	**Response**	**Action required**	**Action completed**
Has the school got an e-Safety Policy that complies with BCC guidance?			
Date of last review and by who			
Date the school e-safety policy was agreed by governors			
The policy is available for staff in the policy folders in school			
The policy is available for parents/carers on the school website			
Name of the responsible member of the Leadership Team			
Name of the responsible member of the Governing Body			
Name of the Designated Child Protection Coordinator			
Name of the e-Safety Coordinator			
Has e-safety training been provided for both pupils and staff where appropriate?			
There a clear procedure for a response to an incident of concern			
E-safety materials from CEOP and Becta been obtained if appropriate			

All staff sign a Code of Conduct for ICT on appointment			
All pupils aware of the School's e-Safety Rules			
Parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules (Code of Conduct)			
Staff, pupils, parents/carers and visitors are aware that network and Internet use is closely monitored and individual usage can be traced			
Has an ICT security audit been initiated by SLT, possibly using external expertise?			
If personal data is collected, stored and used is this according to the principles of the GDPR?			
Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g., Regional Broadband Consortium, NEN Network).			
The school-level filtering been designed to reflect educational objectives and approved by SLT.			

Appendix 4: Netsmart Code of Practice – Staff

Staff NetSmart Code of Practice

- Staff closely monitor and scrutinise what their pupils are accessing on the Internet including checking the history of pages
- Computer monitor and iPad screens are readily visible for the teacher, so they can monitor what the pupils are accessing
- Pupils have clear guidelines for the content of e-mail messages, sending and receiving procedures
- Pupils only use the Internet when supervised by a teacher or adult
- Pupils are taught skills and techniques to enable efficient and effective use of the Internet
- Pupils have a clearly defined focus for using the Internet and e-mail
- If offensive materials are found (despite using professional filters) the monitor or screen should be switched off, materials confiscated and offensive URLs should be given to the ICT Co-ordinator who will report it to our IT support provider
- Virus protections are essential and will be used
- The recommended ISP (Bucks CC) will check sites visited by schools
- Participating in newsgroups/discussion groups – these groups are open to all therefore be careful! It is recommended that pupils don't use these forums

I have read the NetSmart Code of Practice for pupils and staff

I agree to abide by the Staff Code of Practice.

Name: _____

Signed: _____

Date: _____

Appendix 5: Netsmart Code of Practice – Pupil

Pupils' NetSmart Code of Practice

I'm NetSmart because (please colour in the faces):

- I only use the Internet when supervised by a teacher or adult

- I never tell anyone I meet on the Internet my home address, my telephone number or my school's name

- I never send anyone my picture

- I always tell my teacher if I see anything that upsets me

Pupil's Name: .....

I have read the pupil's NetSmart Code of Practice and I have discussed it with my child. We agree to support the school's policy on the use of the Internet.

Signed(Parent/Carer): _____

Date: _____