Hintlesham and Chattisham Church of England Primary School

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

E-Safety and Filtering Policy

Collated by	Mrs Liz Donaldson Executive Head teacher
Approved by **The Local Governing Body**	Hintlesham and Chattisham CE Primary
Signature of Chair of Governors	Deborah Bennett
Date approved	June 2019
Review date	June 2020

***Filtering policy added Nov 2013**
Reviewed January 2014. Password Policy added January 2014
November 2014 revised to include social media.
Revised 2015 to include Prevent duty
Reviewed June 2019
Next date of policy review – June 2020

Hintlesham and Chattisham C of E Primary School
E-Safety and Filtering Policy

This policy document sets out the school's aims, principles and strategies for e-safety, within the school's visions and aims:

Vision

To provide a caring, supportive environment, centred on Christian values, in which every child has the opportunity to achieve his/her full potential.

Aims

At our school we strive to:

- promote a learning partnership between children, parents, teachers and governors
- enable each child to achieve his/her full potential through a broad, balanced and relevant curriculum
- encourage each child to develop a sense of self-esteem, self-discipline, personal responsibility and respect for others
- maintain strong links with the community and ensure that the school continues to be seen as an essential future asset to the village
- promote spiritual awareness and respect for all other religions and cultures
- provide a stimulating, safe and secure environment, which fosters a sense of pride and ownership in the school
- provide a broad range of challenges and experiences in order to enhance the confidence, knowledge and skills of our children

How we ensure this policy meets our duty under the Prevent Strategy (Section 26 of the Counter-Terrorism and Security Act 2015)

The school recognises its duty to protect our pupils from indoctrination into any form of extreme ideology which may lead to the harm of self or others. This is particularly important because of the open access to electronic information through the internet. The school aims to safeguard children through educating them on the appropriate use of social media and the dangers of downloading and sharing inappropriate material which is illegal under the Counter-Terrorism Act.

The school vets all visitors carefully and will take firm action if any individual or group is perceived to be attempting to influence members of our school community, either physically or electronically.

Our definition of radical or extreme ideology is 'a set of ideas which could justify vilification or violence against individuals, groups or self.'

Staff are trained to be vigilant for spotting signs of extremist views and behaviours and to always report anything which may suggest a pupil is expressing opinions which may cause concern. Staff now to report these concerns to the Designated or Deputy Designate Person for Child Protection. We place a strong emphasis on the common values that all communities share such as self-respect, tolerance and the sanctity of life. We work hard to broaden our pupils' experience, to prepare them for life and work in contemporary Britain. We teach them to respect and value the diversity around them as well as understanding how to make safe, well-considered decisions.

Introduction

- Our school e-safety co-ordinator is The Headteacher [also Designated Safeguarding Officer].
- Our e-safety governor is Deborah Bennett [Interim as safeguarding governor].

Teaching and Learning

The internet is an essential element of twenty first century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience. Internet use is part of the curriculum and a necessary tool for staff and pupils. Children in all year groups use the internet when appropriate in curriculum time, and at some clubs, for example at Homework Club, which is supervised by adults. Children are not allowed to use the internet at other times.

Ways in which internet use enhances learning

- The school internet access is designed for pupil use and includes filtering* appropriate to the age of the pupils.
- Children are taught acceptable ways of internet use and are given clear objectives for internet use.
- Children are taught effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children are shown how to present information to a wider audience.

***Filtering**

The filtering of internet content provides an important means of preventing users from accessing material that is illegal and inappropriate in an educational context. The school subscribes to a filtering system provided by CPW, which maintains our school network. However, the filtering system can not, provide 100% guaranteed service. Therefore as part of the e-safety policy this section sets out to manage the associated risks and to provide preventative measures which are appropriate to our school. Filtering is one element in a strategy for e-safety and acceptable use.

The responsibility for the management of the filtering system lies with the e-safety co-ordinator. However, all users have the responsibility to report to the e-safety co-ordinator any infringements of the school's filtering policy. This includes the accessing of any sites which they believe should have been filtered.

Users must not attempt to use any programs or software that might allow them to bypass the filtering systems in place to prevent access to such materials. The e-safety co-ordinator must make staff aware of this policy.

It is the class teacher's responsibility to ensure that the pupils are aware that the school uses filtering systems to prevent access to inappropriate material. Pupils should learn that should they access anything which makes them feel uncomfortable they need to use 'Hector Protector' to cover the screen whilst they report the incident to an adult. Pupils should be encouraged to report all materials which breach their filtering system, including at home.

Ways in which children are taught how to evaluate internet content

- The school will ensure that the use of the internet, by staff and children, complies with copyright law.
- Children are taught the importance of cross-checking information before accepting its accuracy.
- If children come across any internet content that they find worrying, they are taught to use 'Hector Protector' to cover the screen and to report the problem to an adult.
- If members of staff come across unsuitable online materials, the site must be reported to the e-safety co-ordinator.

Published Content and the School Website

- Staff or children's personal contact details will not be published. The contact details given online are the school office.
- The headteacher will take overall responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils are selected carefully, so that everything possible is done to prevent their image being misused, e.g. group photos are often used.
- Children's names are not used anywhere on the school website or other online space, particularly in association with photographs.
- Children's work can only be published with the permission of the pupils and parents.
- Parents are clearly informed of the school policy on image taking and publishing.

Social Networking

- The use of social networking sites is not part of our school curriculum.
- As a school, we accept that some of our children will engage in electronic social networking out of school hours. It is therefore part of our curriculum to teach safe use of social networking sites.
- Children will be advised never to give out personal details which may identify them, their friends or their location.
- Children and parents will be advised that the use of social network spaces outside school brings a range of dangers for children.
- Parents have been provided with documentation, e.g. 'Stop, Think, Stay Safe – How to Protect you and your Family on the Internet.'
- The school will use Family Learning materials in Years 5 / 6, to educate children and parents about e-safety, including the use of social networking sites.

Mobile Phones

See separate policy.

Cameras

- Children only use cameras under adult supervision. They are not allowed to use their own cameras in school. They are taught not to take images of people without their permission. Staff are not permitted to use their own cameras for school activities, either on or off the premises.

Protecting Personal Data
Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998. See Data Handling and Confidentiality Policies.

***Password Security Policy**
The School is responsible for ensuring that the school computer network is safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another person's files without permission
- access to personal data is securely controlled. (Reference Data Handling and Confidentiality policies)

A user name and password system is used so that the above principles are adhered to.

The management of the password security system is the responsibility of the Headteacher and may be maintained by technicians employed by the school. All adults using the computer network are responsible for the security of their username and password and must not allow other users to access the system using their log-on details.
If a child has his/her own password for school centred / initiated programs class teachers may keep a record of the password/username.
Children are monitored to ensure safe working practice when accessing files. Any alleged or actual breaches of security must be reported to the Headteacher. The incident will be recorded and followed up, with reference to the Positive Behaviour and Anti-Bullying Policy if appropriate.

Authorising Internet Access

- All members of staff must read and sign the 'Staff Code of Conduct for ICT.'
- The school maintains a current record of all staff, pupils, volunteers and governors who are granted access to school ICT systems.
- At KS1 and EYFS, access to the internet is by adult demonstration with directly supervised access to specific, online materials.
- Parents and children are asked to sign and return a consent form before the children can use the internet in school.
- Any person not directly employed by the school is asked to sign an 'Acceptable Use of ICT' form before being allowed to access the internet from the school site.

Assessing Risks

- The school takes all reasonable precautions to prevent access to inappropriate material. However, because of the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.
- The school audits ICT to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is effective.

Handling E-Safety Complaints

- All complaints of internet misuse, on the part of either an adult or a child, are dealt with by the headteacher, if necessary in conjunction with the Local Authority and the Police.
- Complaints of a safeguarding nature must be dealt with in accordance with the school's Safeguarding procedures.
- Children and parents are informed of the complaints procedure.
- Children and parents are informed of consequences for pupils misusing the internet.

Communicating the E-Safety Policy and Procedures

Children

- E-safety rules are posted in all rooms where computers are used and are discussed with children and referred to on a regular basis in lessons across the curriculum.
- E-Safety rules are reinforced in assemblies each term. The community police officer is invited to take occasional assemblies on E-Safety.
- Equal opportunities issues are of the utmost importance. Differentiated activities ensure that all children are appropriately catered for. In the case of a small minority of our children with SEN, the use of a teaching assistant helps ensure that all children understand e-safety at an appropriate level. The TA is well-briefed by the teacher before the lesson / activity takes place.

Staff

- All members of staff have a copy of the school E-Safety Policy.
- E-Safety is discussed as part of the induction of new members of staff.
- E-safety Training is part of the staff CPD schedule

Parents and Carers

- Parents' and carers' attention is brought to the school E-Safety Policy in newsletters and on the school website.
- E-safety is mentioned at one of the parents' induction meetings prior to their children beginning school. This is the responsibility of the EYFS co-ordinator.

Governors

- E-safety is a regular item for discussion at governors' meetings. A section on e-safety / report on cyber bullying will from part of the headteacher's report to the governors.

The Wider Community

- Volunteers who help with ICT are given a copy of our E-Safety policy.
- A copy of our E-Safety Policy is sent to the Parish Council, as we recognise that liaison with local organisations will help establish a common approach to e-safety within the wider community.
- Contractors and visitors are given an acceptable use guide.

January 2014 (*Filtering policy added Nov 2013;Password Policy added January 2014) 2014 revised to include social media.
Revised 2015 to include Prevent duty
Next date of policy review – June 2020