



## Cornerstone Church of England (VA) Primary School



*Building our Community  
with Love, Forgiveness and Hope*

### E-Safety Policy

<b>Reviewed by</b>	Resources Committee	<b>Authorised by</b>	Resources Committee
<b>Last Review</b>	Spring 2017	<b>Date</b>	
<b>Next Review</b>	Spring 2018	<b>Review Cycle</b>	Annually

#### Principles (Values)

The internet and devices that utilise it are now part of everyday life for most people and a powerful and useful tool for pupils' learning. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning. Use of the internet is also part of the Computing National Curriculum.

Staff and other adults working with pupils show **Love** in the care and vigilance they take to ensure the pupils stay safe online. They also show this in the way they model and teach the pupils to be respectful and responsible towards other in their use of technology.

They show **Forgiveness** in the way we help pupils learn from mistakes or errors of judgement they may make and to learn to be safer and more responsible in the future.

They demonstrate **Hope** in the way they expect people to use technology safely and responsibly and promote the positive uses of the internet and technology.

#### Aims

All pupils will:

- learn to use the internet and other digital technologies safely and responsibly
- use the internet and other digital technologies to support, extend and enhance their learning
- develop an understanding of the uses, importance and limitations of the internet and other digital technologies
- develop a positive attitude to the internet and develop their ICT capability and confidence through both independent and collaborative working
- develop an understanding of intellectual property and copyright

## **Pupils' use of the internet**

All pupils will:

- be taught how to effectively use the internet for research purposes
- be taught to evaluate information on the internet
- be taught how to report inappropriate web content
- use the internet to enhance their learning experience
- have opportunities to engage in independent and collaborative learning using the internet and other digital technologies
- only be permitted to have mobile phones or other personal handheld technology in school with the permission of the headteacher. These pupils will be required to follow the expectations stated in the ICT Acceptable Use Agreement, and sign a pupil-friendly version

## **Staff responsibilities and actions**

All **staff, volunteers, governors and other adults working at the school** must model appropriate behaviour in relation to use of the internet, and must sign the ICT Acceptable Use Agreement before using any information communications technology on site. All staff should:

- contribute to the development of E-Safety policies and practices
- staff ensure that children are supervised when using the internet
- take responsibility for the security of confidential data
- actively teach the pupils about E-Safety during each unit of learning that involves online use
- to regularly teach E-Safety to highlight to the children the importance of being safe on the internet
- explain to children what internet use is acceptable, and will ensure that pupils only access material that is appropriate to their age and maturity
- set clear Learning Aims and expectations of use for internet use during lessons, and ensure that internet use is embedded to support and enhance the whole curriculum
- demonstrate safe access to the web, and ensure that all pupil access is supervised
- deal with E-Safety issues as they arise and be alert to potential issues / risks

## **IT Leader responsibilities**

The IT Leader will:

- review the security of the school information systems and users regularly
- provide guidance and resources to support other staff's use of the internet and digital technologies / devices

## **Headteacher responsibilities**

The Headteacher will:

- assume overall responsibility for E-Safety issues within the school but may delegate the day to day responsibility to an E-Safety Leader

- ensure that developments at Local Authority level are communicated to the E-Safety Leader
- ensure that the Governing Body is informed of e-safety issues and policies.
- make all staff aware that internet traffic can be monitored and traced to the individual user, and that safe, professional conduct is essential
- assume editorial responsibility for all content on the school website, Facebook page, Twitter account and YouTube channel, ensuring that it is accurate, appropriate and accessible
- report any material believed to be illegal to appropriate agencies such as the Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP).

## **Governors**

The Governing Body will:

- appoint an E-Safety link governor who will ensure that it is included as part of the regular review of child protection and health and safety policies
- support the Headteacher and/or designated E-Safety Leader in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment
- ensure that appropriate funding is authorised for e-safety solutions, training and other activities

## **Email**

- Pupils will only use approved school email addresses in school
- Pupils will inform a member of staff if they receive inappropriate or abusive emails
- Access in school to personal email accounts may be blocked if the Headteacher thinks there is any infringement of the ICT Acceptable Use Agreement
- Emails sent to external organisations must be written carefully and professionally

## **Publishing web content**

- The contact details on the school website should be the school address, admin office email address and telephone number
- The website should respect and reflect property rights and copyright
- Images of pupils should be selected carefully and be published only with the consent of the parents/carers and be presented in a way that reduces the opportunities for it to be reused elsewhere
- Pupils' work can be published on website unless parents have specifically asked for it not to be

## **Managing social media**

Children using social media will be advised:

- to discuss their account on an ongoing basis with a trusted adult in their family
- never to give out personal details which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM and email addresses, full names of friends/family, specific interests and

clubs

- not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- not to publish photos of themselves or others online
- not to arrange to meet people who they have met online

School social media:

- The school's Facebook page and Twitter account are managed by the headteacher, in conjunction with the IT Leader and a member of the Governing Body
- All personal information, including names and photos of pupils will only be published with parental consent. In general the least that can be shared the safer the post.
- Any staff blogs run from the school website must be agreed with the Headteacher. The school website should also centrally host any online communications between staff and pupils (e.g. to support home learning tasks)

Staff use of social media

- Staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children
- Staff should make appropriate use of the security settings available
- Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal
- Under no circumstances should any school staff have any pupils or any ex-pupils under the age of 18 as friends on their social networking sites
- School staff are strongly advised not to accept friendships via their social networking with parents, ex-parents and governors. Where staff do accept such friendships, they must not engage in any discussion regarding the school whether expressing personal views or opinions or simply recounting events or stating facts
- School staff are fully entitled to accept friendships with colleagues via their social networking site but should take care in communications exchanged in areas of public access
- Senior staff and those who have line management responsibility are advised to consider the appropriateness of accepting colleagues as contacts on social networking sites
- Staff to share any concerns that may arise on social media with Headteacher

**Internet filtering**

- The school will work with Hampshire County Council's Schools' Broadband Team to ensure that systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL must be reported by the teacher to the IT Leader immediately and access blocked
- The school's broadband access will be filtered according to the age and maturity of pupils.

## **Managing emerging technologies**

New IT applications, both hardware and software, will initially be explored by the IT Leader in consultation with Hampshire County Council's ICT Advisory Team and SchoolCare. Advice will then be put to the Senior Leadership Team, enabling them to assess the educational benefits and potential risks.

## **Training**

The school will ensure that all teaching staff (teachers and learning support assistants) have a basis understanding of E-Safety. Formal training will be provided for key staff. Ongoing dialogue will support an open culture where potential issues are identified, discussed and solutions agreed.

## **Working with parents and carers**

Ensuring that children are able to use the internet safely requires a partnership approach between the school and parents/carers. Consequently, the school will:

- ensure that this policy and the ICT Acceptable Use Agreement are displayed on the school website
- offer occasional E-Safety workshops for parents
- share with parents' materials that will support their understanding of social media
- ask parents to sign a Home School Agreement which incorporates a commitment to safe internet usage
- teach children that safe access to the internet is as important at home as it is at school.

## **E-Safety Complaints**

- Instances of pupil internet or Learning Platform misuse should be reported to a member of staff
- Staff must log incidents reported to them and if necessary refer the matter to a senior member of staff
- Instances of staff internet or other ICT misuse should be reported to, and will be dealt with by, the Headteacher

## **Related policies**

This policy should be read in conjunction with the school's ICT Acceptable Use Agreement, Behaviour policy, Child Protection Policy and Confidentiality Policy. Any complaints relating to E-safety will be managed according to the school's Complaints Policy.

## **E-Safety in Classrooms**

Each term children will be reminded by teachers how to stay safe on the internet. Every classroom will display an E-Safety poster which children can refer to and help guide them in situations.

KS1

# Being Safe on the Internet

When I use an iPad or Laptop I must remember to:-



KS2

# Being Safe on the Internet

When I use an iPad or Laptop I must remember to:-

