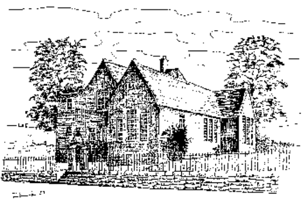
E-Safety Policy

Combe St Nicholas C of E VA Primary School and Pre-School

Name of Policy	E-Safety Policy
Approved by GB - Date	26th April 2016
Next Review Date	25th April 2017
Committee Responsible	Teaching & Learning



This policy should be taken as part of the overall strategy of the school and operated within the context of our vision, aims and values as a Church of England School.

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Combe St Nicholas, we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

This policy sets out the ways in which the school will:

- Educate all members of the school community on their rights and responsibilities with the use of technology.
- Build both an infrastructure and culture of e-safety
- Work to empower the school community to use the internet as an essential tool for life-long learning.

In writing this policy we have taken account of the following:

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger – knowingly or unknowingly-when using the internet and other digital technologies.Indeed, some young people may find themselves involved in activities which are inappropriate or possible illegal."

"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."

From: Safeguarding Children in a Digital World.BECTA 2006

Our e-safety policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The schools e-safety co-ordinator Mr Matt Edwards
- The e-safety governors are Mrs Daphne Lee and Mrs Katherine Stonex
- The e-safety policy and its implementation shall be reviewed annually

It was approved by the governors on (date to be entered) and will be reviewed annually.

E-Safety Policy

Roles and Responsibilities

- Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. The role of the e-safety governor will include:
- Regular Meetings with the e-safety co-ordinator
- Regular monitoring of e-safety incident logs

Headteacher

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-safety co-ordinator
- The Headteacher is responsible for ensuring that the e-safety co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as required
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on more important monitoring roles
- The Headteacher 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
- Use an audit to annually review e-safety (pupils)

The E-safety Co-ordinator

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the e-safety policy/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with school ICT technical support
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality internet access as part of their learning experience:

- The school internet access will be designed expressly for pupil use, including appropriate content filtering
- Pupils will be given clear objectives for internet use and taught what use is acceptable and what is not
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

- As part of the new Computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics like, for example, how to use a search engine, digital footprints and cyber bullying
- The school will ensure that the use of internet derived materials by staff and pupils comply with copyright law

Pupils

- Read ,understand and sign the Pupil and the agree Acceptable Computing User Agreement class internet rules
- Participate in e-safety activities, follow the Acceptable Computing User Agreement d reports concerns for themselves or others
- Understand that the e-safety policy covers actions out of school that are related to their membership of the school

Parents and Carers

- Endorse (by signature) the pupil Acceptable Computing User Agreement
- Discuss e-safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones, and games devices)and the internet
- Access the school website in accordance with the relevant school Acceptable Computing User Agreement
- Keep up to date with issues through newsletters and other opportunities
- Inform the Headteacher of any e-safety issues that relate to the school
- Maintain responsible standards when using social media to discuss school issues

Authorised Internet Access

By explicitly authorising use of the school's internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read and sign the 'Acceptable Computing User Agreement' before using any school computing resource
- Parents will be informed that pupils will be provided with supervised internet access and asked to sign and return a consent form pupil access
- Only authorised equipment, software and internet access can be used within the school

World Wide Web

The internet opens up new opportunities and is becoming an essential part of the everyday world for children: personalized, learning, homework and sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed;

- If staff or pupils discover unsuitable sites the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-safety log, which will be stored in the School office with other safe guarding materials. The e-safety log will be reviewed termly by the e-safety co-ordinator

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- The school will work in partnership with the local authority to ensure filtering systems are as effective as possible

Email

- Ensure that the school uses a secure business email system for communication
- Ensure that personal information is not sent via unsecure email
- Ensure that governors use a secure email system
- Ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- Inform users that if they receive an email that makes them feel uncomfortable,offensive,threatening or bullying in nature to contact the e-safety co-ordinator
- Use emails at KS1 through a group or class activity with an adult sending and opening emails
- Teach KS2 pupils about email safety issues through the scheme of work and implementation of the AUP
- Enable online learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school
- Have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/twitter/YouTube account to share learning experiences
- Staffs are advised that no reference should be made to pupils, parents/carers or school staff
- Advise all members of the school community not to publish specific and detailed private thoughts especially those that may be considered threatening, hurtful or defamatory
- Inform the staff that in the case of a **Critical Incident** they should not make any comment on social media without the permission of the senior management team

Security and Passwords

Passwords should be change regularly. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'

E-Safety Policy

Social Networking

Social networking internet sites (such as youtube, twitter and facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face to face contact.

- Use of social networking sites and personal publishing sites in the school will be filtered
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils
- Pupils will be encouraged to only interact with known friends, family and staff over the internet and deny access to others
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments

Reporting

- All breaches of the e-safety policy need to be recorded in the e-safety log that is kept in the school office. The details of the user, date and incident should be reported
- Incidents which may lead to child protection issues need to be passed on to one of the designated teachers immediately-it is their responsibility to decide on appropriate action not the class teachers
- Incidents which are not child protection issues but may require e-safety coordinator intervention (e.g. cyber bullying) should be reported to e-safety co-ordinator on the same day
- Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff '. If necessary the local authority LADO (Local Authority Designated Officer) should be contacted
- Evidence of incidents must be preserved and retained
- The curriculum will cover how pupils should report incidents (e.g. trusted adult,childline)

Mobile Phones

Many new mobile/smart phones have access to the internet, picture and video messaging, whilst these are more advanced features, they present opportunities for unrestricted access to the internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Inform staff that personal mobile phones should only be used at break, lunchtime and in restricted areas where they are not in contact with pupils, unless they have the permission of the Headteacher
- Inform staff that they are not allowed to use personal devices to take photographs or videos in school for any purpose without the express permission of the Headteacher

- Use of mobile phones in the presence of pupils is not permitted
- The sending of abusive and inappropriate text messages is forbidden
- Staff should always use the school phone to contact parents/carers
- Parents cannot use mobile phones on school trips to take pictures of the children
- On offsite activities and trips, staff mobiles are used for emergency only

Digital/Video Cameras /Photograph

Pictures, video and sound are not directly connected to the internet but images are easily transferred

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff
- Publishing of images, video and sound will follow the policy set out in this document under 'publishing content'
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background
- The Headteacher or a nominee will inform parents/carers and others present at school events that photographs/videos may be taken on the basis that as they are present at a school event photographs/videos may be taken on the basis that they are for private retention only and not for publication in any circumstance
- Staff should always use a school camera to capture images and should not use their personal devices
- Photos taken by the school are subject to the data protection act
- Make sure that pupils full names will not be used anywhere on the school website, particularly in association with photographs, unless permission has been given in advance

Published content and the school website

The school website is a valuable source of information for parents and potential parents

- Contact details on the website will be the school address, e-mail and a telephone number
- Staff and pupils' personal information will not be published
- The Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs, unless permission has been given in advance
- Consent from parents will be obtained before photographs of pupils are published on the school website
- Work will only be published with the permission of the pupil
- Parents should only upload pictures of their own child/children onto social networking sites

- The governing body may ban the use of any photographic equipment by any parent who does not follow the school policy

Protecting Personal Data

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

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content; it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Somerset County Council will accept liability for the material accessed or any consequences of internet access. The school will audit Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff
- Any complaints about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaints procedure
- Where there is cause for concern that illegal activity has taken place or is taking place then the school will contact Somerset Children safeguarding team and escalate concerns to police. Safeguarding School Advisor tel:01823356839

Communication of Policy

Pupils:

- Rules for internet access will be posted in all networked rooms
- Pupils will be informed that Internet use will be monitored
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during computing lessons and all year groups look at different areas of safety through the digital literacy lessons

Staff:

- All staff will be given the e-safety Policy and its importance explained

Parents:

Parents' attention will be drawn to the School e-safety policy in newsletters and on the school website