St Clement's Catholic Primary School

DIOCESE OF ARUNDEL & BRIGHTON

Fennells Mead, Ewell, Epsom, KT17 1TX • Telephone & Fax: 020 8393 8789

Headteacher: Mrs. C. Buckley • www.stclements.surrey.sch.uk

E-Safety Policy

Policy revised by:	ICT Co-ordinator E Safety Co-ordinator
Responsible committee:	Resources
Approved by Governing Body:	Spring 2015
Review Date:	Autumn 2019

OUR MISSION STATEMENT

At St. Clement's Catholic Primary School, we strive to:

- Work in partnership with the home, the parish and the wider community.
- Nurture individuality and foster confidence, independence and self-esteem in a safe and secure environment.
- Engage children in creative, challenging and enjoyable learning experiences, celebrating all achievements.
- Instil respect and promote high standards and positive behaviour in our children.
- Prayer, worship and reflection are central to the spiritual journey of each individual member of our community.

RATIONAL

At St Clement's, we encourage use by all pupils of the rich information and resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. Staff and pupils are encouraged to use this resource well and safely. Wherever possible, staff will select online resources designed specifically for pupil use. At times, the Internet may provide access to information that has not been specifically selected by the member of staff. At St Clement's, the Internet is filtered by an Internet Service Provider who, at all times, will try to ensure that pupils do not access any inappropriate and unwanted information.

AIMS

- To provide an environment in which children feel safe, secure, valued and respected; and feel confident, and able to approach adults with issues of concern.
- To raise awareness in children when using the Internet and equip them with the skills and knowledge when faced with an E-safety issue.
- To raise awareness in parents to the dangers of Internet usage.
- To raise the awareness of all teaching and non-teaching staff of the need to safeguard children and of their responsibilities in identifying and reporting possible cases of abuse.
- To encourage a culture of respect and understanding when using the Internet, especially when using social network sites.
- To develop and promote effective working relationships with other agencies, especially the Police and Social Services.

PROCEDURES

- The Computing Leader will act as e-Safety coordinator.
- All members of staff are provided with opportunities to receive e-safety training, to develop their understanding of the risks to children.
- We recognise that staff working in the school who have become involved with a child who has suffered harm, or appears to be likely to suffer harm, may find the situation stressful and upsetting.
- We will support such staff by providing an opportunity to talk through their anxieties with the DCPO and to seek further support as appropriate.

ALLEGATIONS AGAINST STAFF

- All school staff should take care not to place themselves in a vulnerable position with a child. It is always advisable for interviews or work with individual children or parents to be conducted in view of other adults.
- All Staff should be aware of Surrey's Guidance on Behaviour Issues, and the School's own guidance in the Safer Working Practices Agreement.
- We understand that a pupil may make an allegation against a member of staff.
- If such an allegation is made, the member of staff receiving the allegation will immediately inform the Head Teacher.
- The correct procedure will be followed as per the Child Protection Policy.

TEACHING AND LEARNING

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, e.g. for research.

Internet use will enhance learning

- The school Internet access is provided by BT Unicorn and includes filtering appropriate to the age of pupils. The school uses *Smoothwall* software under contract to BTGS to filter all internet access.

As part of the new Computing Curriculum we will continue to ensure that:

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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 shown how to publish and present information appropriate to a wider audience.
- Pupils will be taught how to evaluate Internet content.
- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

MANAGING INTERNET ACCESS

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

Social Networking

- The school recognises that many staff will actively use *Facebook*, *Twitter* and other such social networking, blogging and messaging services, including to support their own professional development by developing personal learning networks with other educational practitioners.
- Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks – discretion and professional conduct is essential. They are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.
- In accordance with school's *Child Protection Policy*, it is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friend requests from ex-pupils who are still minors to again avoid any possible misinterpretation of their motives or behaviour which could be construed as grooming.
- Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. All correspondence should be via school systems.
- Parents should be aware that a lot of social networking sites are aimed at adults and adolescents over the age of 13 and are therefore unsuitable for children in primary school. It should be advised to parents that they monitor their children's use of the Internet and be aware that allowing their children to access such sites may lead to inappropriate behaviour or online bullying, which the school do not take responsibility for. There are alternative social networking sites specifically aimed at children.

E-mails

- **Pupils may only use approved e-mail accounts on the school system.**
- **All teaching staff should have an approved e-mail account, which should be used as a primary contact for educational purposes.**
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communications or arrange to meet anyone.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Mobile Phones

- Only Year 6 children who walk to and from school by themselves are permitted to bring a mobile phone into school in order to contact parents / guardians on arrival or when leaving school.
- It is recommended to parents that phones should not have access to the Internet. If it does have access, then parents are to be advised that any inappropriate use occurring outside of school hours should be dealt with the parents / guardians. Both the children and their parents will be informed of this at the beginning of the academic year.
- During school time, mobiles are to be kept in the office, managed by the class teacher.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or learning platform.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or learning platform.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Managing filtering

- The school will work in partnership with Surrey County Council 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 e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Video conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the pupils' age.

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.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.

- Games machines including the Nintendo Wii, Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use. Staff should ensure that the use of the Wii within After School Club does not allow internet access.
- Staff will use a school 'phone where contact with pupils is required.
- The appropriate use of Learning Platforms is discussed regularly with pupils throughout the school and annually with parents.

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 for ICT ' before using any school ICT resource (Appendix 2).
- Parents will be asked to sign and return a consent form for the use of internet access within school as well as making them aware of Internet safety at home (Appendix 3).
- Children are asked to sign their own 'Rules for using the Internet Safely' (Appendix 1).

Assessing risks

- 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 SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- 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.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school e-safety policy.

COMMUNICATIONS POLICY

Introducing the e-safety policy to pupils

- Appropriate elements of the e-safety policy will be shared with pupils.
- E-safety rules will be posted in the ICT suite.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils.

Staff and the e-Safety policy

- All staff will be given the School e-safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' 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.
- Parents and carers will be provided with additional information on e-safety from time to time and have permanent access to the e-safety pages via the school's learning platform.

Other Policies

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Bullying, Racist Incidents, Child Protection and Health and Safety.
They reflect the consideration we give to the protection of the children in our care. We acknowledge that to allow or condone bullying or racism may lead to consideration under Child Protection procedures.

Prevention

We recognise that the school plays a significant part in the prevention of harm to our pupils by providing pupils with good lines of communication with trusted adults, supportive friends and an ethos of protection.

The school community will therefore:

- Establish and maintain an ethos where children feel secure and are encouraged to talk and are always listened to.
- Ensure that all children know there is an adult in the school whom they can approach if they are worried or in difficulty.
- Provide lessons to all pupils, strictly devoted to e-safety as well as including it across the curriculum, which equip children with the skills they need to stay safe from harm and to know to whom they should turn for help.
- Promote the school's own e-safety rules and ensure that children are aware of them and that they are displayed throughout the school.
- Parents will be informed of the policy and its practices and a copy of the policy made available for inspection.

Review and Evaluation

The issue of e-safety will be central to the task of review. This policy was written, building on good practice and following consultation with all staff and governors. It will be monitored for effectiveness and updated annually in the light of experience.

APPENDIX 1
Children's Rules for using the Internet safely

Rules for using the Internet safely

I will:

- Ask permission from a member of staff before using the Internet;
- Only visit websites suitable for children my age;
- Be polite and show respect when communicating with others;
- Keep my personal information private (including name, address, telephone numbers and passwords);
- Never agree to meet someone I have met on the Internet;
- Report any unpleasant messages/inappropriate websites to a member of staff.

My Name: _____
My Signature: _____
Date: _____

APPENDIX 2
Staff Code of Conduct for ICT

St Clement's Catholic Primary School

Staff Code of Conduct of ICT

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 policy for further information and clarification.

- I understand that it is a criminal offence to use school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without permission from the head teacher.
- I understand that my use of school information systems, Internet and e-mail 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 manager.
- I will not install 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.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-safety co-ordinator the designated child protection officer or head teacher.
- I will ensure that electronic communications with children including e-mail, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted
- I will promote e-safety with children 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 ICT systems to intercept e-mail and delete inappropriate materials where it believes unauthorised use of the schools 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.

Name: ……. Signed: ……

Date: ……..

Head teacher: …… Date: ……

APPENDIX 3

St Clement's Catholic Primary School

DIOCESE OF ARUNDEL & BRIGHTON

Fennells Mead, Ewell, Epsom, KT17 1TX • Telephone & Fax: 020 8393 8789

Headteacher: Mrs. C. Buckley • www.stclements.surrey.sch.uk

Safe Use Agreement for Parents/Guardians for Internet Use

Dear Parents,

As part of the new National Curriculum and the development of computing skills, e-safety is an imperative part to our children's learning, understanding and well-being within both computing lessons and in their daily lives.

Please would you read the attached *Rules for using the Internet Safely* that children need to sign, then sign and return the attached consent form.

In school, we take positive steps to dealing with any e-safety concerns, including making children aware of the e-safety rules and how to keep themselves safe during computing and PSHE lessons as well operating filtering system that restricts access to inappropriate material. Furthermore, websites that are deemed inappropriate are blocked.

This may not however be the case at home and we would strongly recommend for you to monitor your child's Internet use and apply parental controls where available.

We suggest you consider the following:

- Keeping the computer / laptop / tablet / phone to which children are accessing the Internet in a communal area of the home;
- Ask your children how the computer and Internet work;
- Monitor on-line time and be aware of excessive hours spent on the Internet;
- Take an interest in what your children are doing by discussing with them what they are seeing and using on the Internet, including what is inappropriate material and how they should respond to unsuitable material or requests;
- Be mindful that although a lot of social networking sites are aimed at adults and adolescents over the age of 13, some children below this age have accounts and are regularly using them. This may lead to accessing inappropriate material or behaviour and occasionally, bullying. If such matters arise, it is not the school's responsibility to deal with them.
- Be aware that children may be using the Internet in places other than in the home or at school;
- Be aware of the safety issues of mobile phones as well as game consoles that have access to the Internet. If supplying a mobile for your child, if they are walking to and from school by themselves (Year 6 only), we advise that you choose one that has no Internet access or where access can be restricted. Please note that if children consistently use their phones inappropriately, i.e. by accessing the Internet or such like, the privilege to bring a phone onto the school premises will be revoked. During school time, all mobiles should be handed to their class teacher, which are then kept in the office.

There are many websites now available which help you to understand more about e-safety at home, including those that are accessible on Fronter:

- **CEOP Think You Know** - https://www.thinkuknow.co.uk/parents
- **Childnet International** - http://www.childnet.com/parents-and-carers
- **Hertfordshire Grid for Learning** - http://www.thegrid.org.uk/eservices/safety/parents.shtml
- **UK Safer Internet Centre** - http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls

For further information, please see our E-Safety Policy, which is available on our website.

Safe Use Agreement for Parents/Guardians for Internet Use

Pupil Name(s): _____ Class(es): _____

As the parent or legal guardian of the above pupil(s), I give my permission for my son or daughter to have access to the Internet in school.

I have read both the *Rules for using the Internet safely* and the *Safe Use Agreement for Parents/Guardians for Internet Use from the school's E Safety policy* and I support my child and the school in developing safe and responsible use of the Internet.

Parent/Guardian Signature: _____
Date: _____

Appendix 4:

Further Points for Children to Consider

Follow these SMART tips

Secret - Always keep your name, address, mobile phone number and password private - it's like give out the keys to your home!

Meeting someone you have contacted in cyberspace can be extremely dangerous. Only do so with your parent's carer's permission, and only when they can be present.

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages.

Remember someone on-line may be lying and not be who he or she say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

Tell your parent or carer if someone or something makes you feel uncomfortable or worried.