

Cottesmore St Mary Catholic Primary School

E-Safety Policy



'Manus nobiscum Domine'
(Abide with us O Lord)

Date of policy review: November 2016

Next review: November 2019

Policy written by: Fiona Merritt (all staff consulted)

Policy reviewed & passed by: PPCC committee

Key people responsible for Computing: Fiona Merritt

Other policies linked to this policy:

- EPR
- Anti-bullying
- Child Protection Policy
- Teaching and Learning Policy
- Anti-bullying Policy
- Behaviour Policy
- Photographic & Video Images Policy
- Use of Social Media Policy

CONTENTS

Mission statement - Page 3

Context – Page 4

Expectations of staff – Page 5

Expectations of children and e-safety week – Page 6

Parental support, e-safety contacts and references – Page 7

Appendices

Letter to parents about use of computer games – Page 8

Internet safety rules – Page 9

Our Mission

God made each one of us, we are all His disciples.

We believe in ourselves and help each other to do our best, respecting each other's differences and including everyone. We show care for others, especially by helping those in need and acting as God wants us to whilst living the Gospel daily.

We pray and worship together and so grow closer to God and each other, celebrating when others do well. We are part of God's family, supporting other people in school, at home, at church and in the world around us.

Mane nobiscum Domine - Abide with us Lord.



We want the children who leave our school to make the most of every learning opportunity so that they can grow into the best people they can be, fulfilling their dreams and God's special plan for them, being happy and confident and joyfully showing to others their faith in God.

Context

Internet use is part of the statutory curriculum and a necessary tool for learning. The National Curriculum (2014) requires that children:

- Use technology safely and respectfully
- Know how to get help and support when they have concerns about content or contact

For further details of Computing curriculum expectations at each key stage see:

www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study

Children and staff rely on swift and easy access to the internet for a wide range of valid and valuable purposes; its use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

There are potential dangers posed by use of the internet and other multimedia resources; this policy is written to explain how we manage these risks for children. The school will take all reasonable precautions to ensure that children access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the local authority can accept liability for the material accessed, or any consequences resulting from Internet use. The use of school computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Any complaint about staff misuse must be referred to the head teacher. The school is aware that bullying can take place through social networking especially in open access areas without password protection where anyone can view the bully's comments. The school will be sensitive to Internet related issues experienced by pupils both in and out of school and offer appropriate advice. EPR lessons and computing lessons address internet safety and cyber bullying.

Our e-Safety Policy has been written by the computing subject leader, with advice and guidance from the Schools ICT dept at Brighton and Hove City Council, e-Safety organisations and central government. It should be read in conjunction with other school policies available on the school website

The school's designated person for Child Protection is Rachel Kershaw and the e-Safety Coordinator is Fiona Merritt. Angela Pinnell is the registered Data Protection Officer who is responsible for data security at the school.

This policy has been agreed by the senior management team and approved by the school's governing body. The E-Safety Policy and its implementation will be reviewed annually.

Expectations of staff

- E-safety is taught as part of the Computing National Curriculum (2014). This includes the reasons for caution in publishing personal information and images in social publishing sites and instruction in responsible and safe use preceding Internet access. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and ensure that pupils are aware that their network and Internet use will be monitored, as for all their other school work.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, teacher approved on-line materials. By the end of KS1 children should be taught how to '*use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies*'. (NC 2014)
- At Key Stage 2, access to the Internet will be by adult demonstration and supervised direction to age appropriate on-line materials. By the end of KS2 children should be taught to '*understand computer networks including the internet... use search technologies effectively ... use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.*' (NC 2014)
- All staff are given the School e-Safety Policy. Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.
- Staff are aware that Internet traffic can be monitored and traced to the individual user. It is essential that teachers exercise their professional discretion and conduct in line with their contract of employment. Teachers may operate moderated online posts (e.g. blogs or wikis) as part of their teaching activities. These must be password protected and run from the school network. Teachers are advised not to run social network spaces for pupil use on a personal basis.
- Any material found on the school network and associated devices that the school believes is illegal may be reported to appropriate agencies such as the Internet Watch Foundation (<https://www.iwf.org.uk>) or the Child Exploitation & Online Protection Centre (<http://www.ceop.police.uk>).
- The school currently filters Internet access using Smoothwall (Jan 2015). The ICT team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or pupils discover unsuitable websites via the school network, the URL must be reported to the E-Safety Coordinator or a senior manager to ensure that the filtering systems are updated. Children are taught to minimise rather than close such sites that they might discover to aid in this process.
- Digital communications sent by pupils to external organisations will be prepared carefully and authorised by a teacher, before sending, in the same way as a letter written on school headed paper.
- Pupils' full names will not be published online e.g. on the school's website, Images that include pupils will be selected carefully so that individual pupils may not be clearly identified. Written permission from parents or carers will be obtained before images of pupils are electronically published by the school. This is carried out as part of the admissions process.

Expectations of Children

Internet access is available for all pupils providing they show a responsible and mature approach to its use. Children who consistently demonstrate a positive attitude and aptitude for Computing will be nominated as Digital Leaders in their class. If internet access is purposefully misused sanctions within the school behaviour policy include interview/counselling by senior staff; informing parents or carers and may require removal of Internet or computer access for a period.

Children will learn to:

- Protect their personal information and keep it private, not share it with strangers and to ask a trusted adult if not sure.
- Be kind online. Tell a trusted adult if anyone is being mean online.
- Use Internet enabled devices as instructed by school staff. Hand in their own devices (e.g. phones, tablets etc.) to their class teacher on arrival.
- Immediately minimise or hide from view anything online that worries or concerns them and tell a teacher.
- Meet online friends with a trusted adult.
- Ask for permission to use copyrighted materials.
- Check the accuracy of online materials and information, as anyone can upload information of any quality.
- Internet safety rules are displayed in the computer suite and on the school website. E-safety posters are on display by all fixed devices with Internet access in classrooms and the Computer Suite and should be referred to for guidance. See Appendix 2.

E-safety week

- The school holds an e-safety week annually following guidance from <http://www.saferinternet.org.uk/> with whole school assemblies, in class activities and competitions where children are asked to design items to promote the awareness of safety e.g. a mouse mat, screen saver or a poster.
- There is also an annual e-safety workshop for parents organised by Safety net.

Parental Support

A partnership approach with parents and carers is encouraged in all areas of school life. As part of e-Safety this could include parent evenings with demonstrations, suggestions for safe home Internet use posted on the school website and focus e safety weeks at school.

Parents are asked to read the school's e-Safety Policy and are invited to ask for clarification or advice on any of the points; the best piece of advice from all agencies is for parents **to share and be aware** of their child's online activities, much as you would in any other public space. Parents are asked to sign and return a consent form for pupil Internet access as part of the admissions process.

Parents and carers are asked to work in partnership with school staff to resolve issues of e-Safety so that they may be handled sensitively. However, parents need to be aware that in rare serious cases discussions may be held with the local Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

E-Safety Contacts and References

This is not an exhaustive list but contains sites that offer advice to parents and some which have child centred activities that may be used in school.

CBBC Stay Safe	www.bb.co.uk/cbbc/topics/stay-safe
Childline	http://www.childline.org.uk
Childnet:	www.childnet.com
Click Clever Click Safe Campaign	http://clickcleverclicksafe.direct.gov.uk
Cybermentors:	www.cybermentors.org.uk
NAACE – National association for technology in education	www.naace.co.uk
National Education Network	www.nen.gov.uk
Action for Children	www.actionforchildren.org.uk
NSPCC	www.nspcc.org.uk
Parent Zone – Digital Parenting Mag	www.theparentzone.co.uk
Safety Net	www.safetynetkids.org.uk , www.safety-net.org.uk
Child safeguarding	pansussexscb.proceduresonline.com/index.htm , www.brightonandhovelscb.org.uk
Think U Know website	www.thinkuknow.co.uk
West Sussex e-Safety Pages	www.westsussex.gov.uk/learning/west_sussex_grid_for_learning/management_info_services/it_support_for_schools/e-safety_in_west_sussex_school.aspx
Working Together to Safeguard Children (March 2013)	www.workingtogetheronline.co.uk
Virtual Global Taskforce – Report Abuse	www.virtualglobaltaskforce.com
NAACE – National association for technology in education	www.naace.co.uk
National Education Network	www.nen.gov.uk
Action for Children	www.actionforchildren.org.uk

April 2015

Dear Parents/ Carers,

Our Duty of Care regarding Computer games

One of the issues that increasingly arises in children's time with our school counsellor, and in class and playground discussions is that of computer games. More and more children are telling us that they play games such as 'Call of Duty' and 'Grand Theft Auto' at home, either on their own or with older siblings or adults. These games carry an '18 Certificate' because they have a highly violent and sexual content as well as themes around criminality. Unlike games designed for young children, the graphics are very realistic. Exposing children to this kind of material and allowing them to witness simulated acts of violence plus content of a sexual nature can be very detrimental to their emotional and behavioural development. Research now seems to be showing that children who are allowed to play adult games are more likely to display violent and sexualised behaviour. Here are some links to research articles on the possible effects of violent video games on children:

<http://www.nature.com/tp/journal/v1/n11/full/tp201153a.html> The Neural basis of video gaming

<http://www.ncbi.nlm.nih.gov/pubmed/22040315> A longitudinal study of the association between violent video game play and aggression among adolescents

<http://dx.doi.org/10.1093/acprof:oso/9780195309836.001.0001> Violent video game effects on children and adolescents: Theory, research, and public policy.

We know it can be really difficult to monitor what our children are allowed to play, especially as they may have access at other children's houses or because of peer pressure, but we feel strongly that it is incumbent on us all to be increasingly vigilant against the 'normalisation' of this kind of material affecting our children's lives. Here are some links to sites that help you to set-up parental controls on general internet use:

<http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls>

<http://www.google.co.uk/safetycenter/families/start/>

<https://www.thinkuknow.co.uk/parents/Primary/Tools/Parental-controls/>

If you would like to discuss any aspect of this then please talk to your child's form teacher or Rachel Kershaw, Deputy Headteacher and SENCO.

Many thanks,

Rachel Kershaw
Deputy Headteacher

Be smart on the internet

Childnet International
www.childnet.com

S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

t TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

KidSMART Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

THINK UK KNOW .co.uk

Childnet International © 2008 Registered Charity no. 1086172