St Augustine’s RC Primary School
Online Safety Policy

SERVITE DOMINO IN LAETITIA

ST AUGUSTINE'S
CATHOLIC PRIMARY SCHOOL

‘Serve the Lord in gladness’

Articles- 4,5,8,16,19,28,36

Online Safety Policy

Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's Online Safety Policy will operate in conjunction with other policies including Child Protection, Safeguarding Behaviour, Anti-Bullying, Curriculum and Data Protection.

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.
- National Education Network standards and specifications.

Writing and reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- The school will appoint an Online Safety Coordinator as part of the Designated Safeguarding Lead role as the roles overlap. It is not a technical role.
- Our Online Safety Policy has been written by the school and has been agreed by senior management and approved by governors.
- The Online Safety Policy was revised by: Matthew Robbins
- The next review date is (at least annually): September 2022

Teaching and learning

Why the Internet and digital communications are important:

The purpose of Internet 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 information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This is controlled by the academy trust (NPCAT)
- 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 to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon and SMART approach.

Managing Internet Access:

Information system security

- School IT systems security will be reviewed regularly.
- Virus protection will be updated regularly by Trust technicians.
- Security strategies will be discussed with the Local Authority / NPCAT IT support.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

Google Classroom (online educational platform)

- Pupils will use their real name and an appropriate avatar or picture of themselves in order to stay safe online.
- Teachers and pupils will use the platform responsibly, only uploading school related information and tasks- modelling and promoting Standard English.
- Google Classroom will be used only as a learning/educational platform.

Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The head teacher 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 so that individual pupils cannot be identified, or their image misused unless parental consent has been given. Where possible, group photographs rather than full-face photos of individual children will be used.
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or social media channels.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. (Children will not be able to access social networking sites within school.) - Newsgroups may be blocked.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work with Middlesbrough LA and NPCAT IT support 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 (DSL)/ HT / DHT.
- Senior staff/ Academy Trust will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use 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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- In direct response to this, mobile phones are not permitted in classrooms by pupils, staff and visitors. They are locked away in designated lockers.
- Staff will be issued with a school phone and or image taking device where contact with pupils is required or where mobile phones are used to capture photographs of pupils.

Protecting personal data

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

- **The Data Protection Act 2018** is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is: used fairly, lawfully and transparently.

Policy Decisions:

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign an "acceptable use policy" before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to 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. Neither the school nor Middlesbrough LA/ NPCAT Trust can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

Handling Online 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 when necessary (see schools complaints policy)

- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- The school will liaise with local organisations/Trust to establish a common approach to online safety.

Introducing the Online Safety Policy to pupils

- Online Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in Online Safety will be developed, possibly based on the materials from CEOP.
- Online Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) and JIGSAW curriculum.

Staff and the Online Safety Policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.
- The contact details on the Web site should be the school address, email and telephone number. Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- All staff are aware of the PREVENT Strategy and will monitor the use of the internet in conjunction with the NPCAT IT team (IT provider) to protect children from accessing website material linked to extremism /

radicalisation. All the staff at St Augustine’s School have received their Child Protection Basic Awareness Training as well as ‘Safeguarding in Education’ training. Teaching and teaching support staff have also completed the Channel General Awareness course in relation to PREVENT.

- Headteacher Mrs Rehbohm and Mr Macauley are the Designated Safeguarding Lead (DSL) and Mrs Dunning and Mrs Nicholson are Deputy Designated Safeguarding Leads (DDSL).

Enlisting parents’ and carers’ support

- Parents and carers attention will be drawn to the school Online Safety Policy in newsletters, the school brochure, Google Classroom and on the school website.
- The school will maintain a list of e-safety resources for parents/carers.

Key Stage 1
‘Think then Click’

These rules help us to stay safe on the Internet:

- We only use the internet when an adult is with us
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can send and open emails together.
- We can write polite and friendly emails to people that we know.
- Think SMART!

Key Stage 2
‘Think then Click’

E-Safety Rules for Key Stage 2:

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.
- Think SMART!