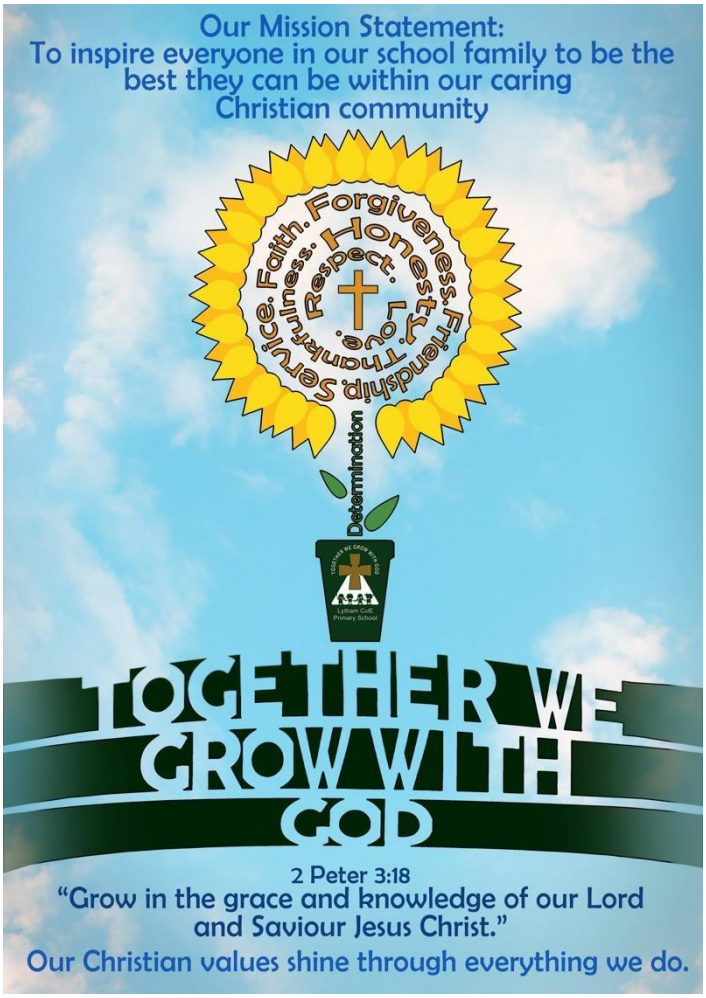
Lytham Church of England Primary School

Online & Digital Safety Policy



Subject Leader: Mrs. K. Coster-France
Linked Governor: Mrs. M. O'Neill
Date of Policy: October 2021
Date of Review: October 2022; October 2023

Together We Grow with God

Mission Statement

To inspire everyone in our school family to be the best they can be within our caring Christian community.

Online safety encompasses internet technologies and ALL electronic communication devices including mobile phones and tablets. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguarding and an awareness for users which enables them to control their online experience.

This policy should be read in conjunction with other policies including our Child Protection and Safeguarding policy; Our Behaviour Policy; Our GDPR policy; as well as our Code of Conduct for the use of online resources.

The school's online safety Coordinator, at the time of this review, is the Computing Subject Leader: Mrs. K. Coster-France.

It has been agreed by the Senior Leadership Team and ratified by governors.

This Online Safety Policy will be reviewed every year to keep up to date with evolving technologies and programmes.

Teaching and Learning

- The Internet is an essential element in 21st century life for education, business and social interaction.
- Lytham CE Primary School recognises that it has a duty to provide children and young people with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool in teaching and learning for staff and pupils.
- The schools internet access is available to enhance the teaching and learning in school. It is designed expressly for pupil use and includes BTLS filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Staff will also educate them in the effective use of the internet for research, including the skills of knowledge location, retrieval and evaluation. It is important that pupils learn not to copy information from the internet (plagiarise) but use it to inform their writing.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to: BTLS ICT Services, and the school e-safety officer.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly – by Western Technician Service.
- The school uses BTLS with high level security firewall and filters.

E-mail & Digital Communication (Office 365, ClassDojo, Google Classroom)

- Pupils may only use approved e-mail accounts on the school system.
- Pupils are educated to immediately tell an adult if they receive offensive e-mail or other forms of negative digital communication.
- Pupils must not reveal personal details of themselves or others in digital communication.
- E-mail from staff members sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- On the school website, the Computing Lead and Assistant Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Staff and Pupils' Images and Work

- Photographs that include pupils will be selected carefully (only pupils who have publication approval from parents) and will not enable individual pupils to be clearly identified via their full name being published alongside their photograph.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website and school social media channels – this is carried out as part of the application & induction process for Reception Class pupils and new pupils arriving at school.
- Images of staff will only be published on our school website and social media channels (to the best of our knowledge) with consent.

Social Networking

- Social networking sites will be blocked at all times to pupils. Staff are able to access these for school promotional purposes only (Facebook; Twitter).
- Pupils will be taught never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, name of school, IM address, e-mail address, names of friends, DOB, specific interests and clubs etc.
- The legal requirements around Pupils' access to social media is shared and discussed with the children within our online safety curriculum and any concerns raised would be shared with their parents.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils and parents are signposted to the digital wellbeing section of our school website, as well as other relevant agencies.

Managing Emerging Technologies (e.g. Apple Watch, FitBits, etc.)

- Emerging technologies will be examined for educational benefit before use in school is allowed.
- Mobile phones will not be allowed to be used on school property. If brought to school by the children for safety reasons (walking home alone) the mobile phone must be switched off and handed to a member of staff during the school day.
- Staff may use their mobile phones in the absence of children or during an emergency.
- Staff may only use school provided devices to for use around the children (photographs, etc.) Staff must not use personal devices to take photographs of children.

Handling Online Safety Complaints

- Complaints of Internet misuse by pupils will be dealt with by a senior member of staff. A log of such incidents will be kept on CPOMS, shared with DSL and where appropriate parents will be informed in line with our Safeguarding and Child Protection Policy.
- Any complaint about staff misuse must be referred to the Head teacher or chair of governors who should use the agreed whistleblowing procedures (see Whistleblowing Policy).
- Complaints of a child protection nature will be dealt with in accordance with agreed child protection procedures (see Safeguarding and Child Protection Policy).
- Any sanctions will be in line with our school behaviour policy.

Date: October 2022; Reviewed January 2023