KINGSNORTH CHURCH OF ENGLAND PRIMARY SCHOOL

Name of Policy:	**e-Safety**
Date Written:	**January 2014**
Updated By Who:	**S Sullivan**
Policy Originated from:	**J Tibbles**
Date	**29/1/15 reviewed**
Date To Be Reviewed:	**January 2016**
Policy Approved By:	**Headteacher:**
	Chair Of Governors:
	Governing Group:

STATEMENT OF INTENT

'Recognising its historic foundation, the school will preserve and develop its religious character in accordance with the principles of the Church of England and in partnership with the Church at parish and diocesan level.

The school aims to serve its community by providing an education of the highest quality within the context of Christian belief and practice. It encourages an understanding of the meaning and significance of faith and promotes Christian values through the experience it offers all pupils.'

THE AIMS OF KINGSNORTH CHURCH OF ENGLAND PRIMARY SCHOOL

'This is underpinned by a commitment to guiding our children to an understanding of the Christian Faith.

We aim for them to leave us, having started on a spiritual journey which will enrich and deepen their adult lives.'

'Kingsnorth Church of England Primary School has a strong Christian commitment. We believe through Christian teaching and example children will benefit and be enriched.

We aim to educate children with a firm foundation of Christian knowledge and experience in order to encourage their spiritual development. This means respecting the beliefs and values of other people whether they have a religious background or not.'

INCLUSION AND EQUAL OPPORTUNITIES

This policy should be read while referencing our school's Single Equality Scheme. All children have equal access to the curriculum regardless of their race, gender, or disability. Our behavior policy underpins all that we do at Kingsnorth and should be closely linked to our other policies.

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 functions.

The school's e-Safety Policy will operate in conjunction with other policies including those for pupil Safeguarding, Behaviour, Bullying, Curriculum, Data Protection and Security. The Deputy Headteacher is the e-Safety co-ordinator.

1. AIMS

Ensure the safe and appropriate use of the Internet in order to:

- Raise educational standards;
- Promote pupil achievement;
- Support the professional work of staff; an
- Enhance the school's management functions.

Internet use is part of the statutory curriculum and a necessary tool for learning.
Ensure that students show a responsible and mature approach to its use.
Provide pupils with quality Internet access as part of their learning experience.
Teach pupils to learn how to evaluate Internet information and to take care of their own safety and security

2. THE SCHOOL WILL:

Take all reasonable precautions to ensure that users 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 KCC can accept liability for the material accessed, or any consequences resulting from Internet use

Provide and discuss with all members of staff, the e-Safety policy, ensuring that they are aware that Internet traffic can be traced to an individual user;

Provide staff training in safe and responsible Internet use as appropriate;

Publish the e-Safety policy on the school website and signpost through the use of newsletters and the school prospectus, there will also be copies available at the school office;

Ensure that all stakeholders are aware of and have signed the Acceptable Use Policy and ICT Code of Practice before they are given access to ICT resources; *All stakeholders will read and sign both documents. (Added)*

Block access to social networking sites such as Facebook and Twitter

Ensure that all rooms with Internet access have the e-Safety rules clearly displayed;

Emphasise that cyber-bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying;
Audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate

3. STAFF WILL:

Read and sign the Acceptable Use Policy before using any school ICT resource

Teach a program of e-Safety in the *first, third and fifth* term of each academic year in order to raise the awareness and importance of safe and responsible internet use;

Ensure that at Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific approved on-line materials *and that staff have checked the contents before the pupils access the sites. (added)*

Ensure that any blogs or wikis are password protected and run from the school website.

Ensure that they are professional at all time while using the Internet, both in and out of school.

It is not acceptable for adults to accept or have as a friend ANY pupil on a social media site. Staff who choose to ignore this will be in breach of this school's policy.

Staff will not accept as 'friends' any ex-pupils who are under the age of 18 on any social media site.

Staff should not accept Friends requests/IM conversations on personal profiles of any social media sites, or contact by school email address or store on their personal phones, present parents or past and present pupils, phone numbers/email addresses. Staff who choose to ignore this will be in breach of this policy.

Pre-existing relationships should be discussed with the headteacher.

4. PUPILS WILL:

Only use the Internet under the supervision, and with the consent, of a responsible adult

Report any unsuitable sites to a member of staff immediately;

Be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Never give out personal details of any kind, which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of friends, specific interests and clubs etc.

Not place personal photos on any social network space. They should consider how public the information is and consider using private areas;

5. PARENTS/CARERS ARE ASKED TO:

Sign and return a consent form for their children to be given access to the Internet

Not permit their children to bring mobile phones to school or on school visits, i.e. day-trips or residential visits. (at the present time they do to discuss)

6. EMAIL

Pupils may only use pre-approved email accounts, i.e. whole-class email addresses;

Pupils must not must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult;

Personal staff/governor email addresses should not be used for emails which contain information which has been deemed confidential

7. PUBLISHING DIGITAL CONTENT (SCHOOL WEBSITE & TWITTER)

All content to be published on the School Website or Twitter must first be approved by the Headteacher or Deputy Headteacher;

Staff or pupils' personal information must not be published

Images that include pupils will be selected carefully and will not provide material that could be reused;

Pupils' full names will not be used anywhere on the website, particularly in association with photographs;

Written permission from parents or carers will be obtained before images of pupils are electronically published;

The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright

CIC/LAC children's photographs will not be used on the school web site without written permission of a Social Worker.

8. FILTERING

The school relies of EIS for it's filtering through the accredited KCC provider

The school's access strategy has been designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

The school will work with KCC and Schools Broadband team to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL 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.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

The school's broadband access will include filtering appropriate to the age and maturity of pupils.

9. LEARNING PLATFORMS/ENVIRONMENTS

The school does not currently use any Learning Platforms/Environments

10. VIDEO CONFERENCING

The school does not engage in nor have any equipment to participate in Video Conferencing.

11. PERSONAL DATA

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

12. COMPLAINTS

Complaints of Internet misuse will be dealt with using the School Complaint's Procedure;

Any complaint should be referred to the Headteacher or Deputy Headteacher

Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.

Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

All e–Safety complaints and incidents will be recorded by the school — including any actions taken

13. REVIEW

This policy will be reviewed annually or at any other time if changes are required to comply with changes in legislation, regulation or National or KCC advice;
Any amendments require the approval of the full Governing Body.
The e-Safety Coordinator is Sue Sullivan (Deputy Headteacher)
The Link Governors for e-Safety are Laura Paine and Jim Taggart