St Michael's is an inclusive Church of England School centred on distinctive Christian Values.
We create and provide a high quality, caring and loving educational environment where children can learn, grow and develop to their full potential.

E-SAFETY POLICY

1. Introduction

The school has an appointed E-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap. Our E–Safety Policy has been written by the school, building on the NCC E–Safety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by governors. The E-Safety Policy and its implementation will be reviewed regularly. When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

2. The importance of Internet usage

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. Internet use is part of the statutory curriculum and a necessary tool for learning. Internet access is an entitlement for students who show a responsible and mature approach to its use. The Internet is a part of everyday 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. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

3. The educational benefits of the Internet

Access to world-wide educational resources including museums and art galleries; educational and cultural exchanges between pupils world-wide; professional development for staff through access to national developments, educational materials and effective curriculum practice; access to learning wherever and whenever convenient.

The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4. Teaching pupils how to evaluate Internet content

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of on-line materials is a part of teaching/learning in every subject.

5. Maintaining information systems

Virus protection will be updated regularly. The security of the school information systems and users will be reviewed regularly. Unapproved software will not be allowed in pupils' work areas or attached to email. The ICT co-ordinator / network manager will review system capacity regularly. The school Internet access will be designed to enhance and extend education. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

6. Managing email

Pupils may only use approved e-mail accounts. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult. Access in school to external personal e-mail accounts may be blocked. E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain messages is not permitted. Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team. Staff should not use personal email accounts during school hours or for professional purposes.

7. Managing published content

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

8. Publishing images of pupils

Images that include pupils will be selected carefully and will not provide material that could be reused. Written permission from parents or carers will be obtained before images of pupils are electronically published.

9. Social networking, social media and personal publishing

The school will block/filter access to social networking sites. Pupils will be advised never to 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, IM and e-mail addresses, full names of friends, specific interests and clubs etc. Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school. Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others. Students should be advised not to publish specific and detailed private thoughts.

10. Managing filtering

The school will work with NCC and the 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 (Internet Watch Foundation) or CEOP (Child Exploitation and Online Protection). The school's broadband access will include filtering appropriate to the age and maturity of pupils. The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

11. Managing videoconferencing

Content Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity. Videoconferencing should be supervised appropriately for the pupils' age. Establish dialogue with other conference participants before taking part in a videoconference. All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer. The equipment must be secure and if necessary locked away when not in use. School videoconferencing equipment should not be taken off school premises without permission. Users Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

12. 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 will not be used during lessons or formal school time (as part of the School AUP). The sending of abusive or inappropriate text messages is forbidden.

13. Protecting Personal data

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

14. Authorising Internet access

All staff must read and sign the 'Staff Information Systems Code of Conduct' (see below) or Acceptable Use Policy before using any school ICT resource. At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

15. Assessing risk

The school should audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly. 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 NCC can accept liability for the material accessed, or any consequences resulting from Internet use.

16. Handling E-safety complaints

Complaints of Internet misuse will be dealt with under the School's Complaints Procedure. Any complaint about staff misuse must be referred to the Head Teacher. Pupils and parents will be informed of the complaints procedure. Parents and pupils will need to work in partnership with staff to resolve issues. Discussions will be held with the local Police and/or the Northumberland Safeguarding Children Board 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.

17. Internet usage across the community

The school will liaise with local organisations to establish a common approach to E-safety. The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

18. Managing Cyberbullying

Cyberbullying (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. There will be clear procedures in place to support anyone affected by Cyberbullying. All incidents of cyberbullying reported to the school will be recorded. There will be clear procedures in place to investigate incidents or allegations of Cyberbullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

19. Managing Learning Platforms and Learning Environments

SLT and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities. Pupils/staff will be advised on acceptable conduct and use when using the learning platform. Only members of the current pupil, parent/carers and staff community will have access to the LP. All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

20. Sharing policy with pupils

E-Safety rules will be posted in rooms with Internet access. An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use. Pupil instruction in responsible and safe use should precede Internet access. All users will be informed that network and Internet use will be monitored. E-Safety training will be part of the transition programme across the Key Stages and when moving between establishments. Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

21. Sharing policy with staff

The E–Safety Policy will be formally provided to and discussed with all members of staff. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff training in safe and responsible Internet use both professionally and personally will be provided. To protect all staff and pupils, the school will implement Acceptable Use Policies.

22. Enlisting parental support

Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website. Interested parents will be referred to relevant organisations Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents. Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

St Michael's CE Primary School Declaration:

We confirm that this document is the school's official policy on e-Safety.
This policy should be read in collaboration with the AUP (Acceptable Use Policy)

This document was produced by the e-Safety Policy Document Generator designed for Kent County Council (KCC) by EIS, Maidstone a business unit of KCC

Chair of Governor Committee…2….

Signed: … Jackie Chevaugeon **…………………………………………**

Print Name: …Jackie Chevaugeon… ……………………………………..

Date:………11.7.18 …………………………….

Head teacher

Signed: …… G Johnston **…………………………………………………..**

Print name:……GAVIN JOHNSTON………………………………………

Date: ………11.7.18…………………………………………..

REVIEW DATE … …Summer 2020…………………………..

St Michael's CE Primary School Staff & Governor Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Head Teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure 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 school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's 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 agree with the Information Systems Code of Conduct.

Signed: ……………………………………………… Date: ………

Position: …………………..…………………………….