Cossington C.E. Primary School

'Care, Significance, Purpose'

E-Safety Policy

1. Mission Statement

Care, Significance, Purpose

With a foundation of distinctly Christian Values at our core, Cossington CE Primary School aims to offer an inclusive and inspirational learning environment where every learner is warmly welcomed and can say:

'I am cared for' because God loves me and calls me to care for others.'

'I am significant because God chose to create me and everyone else in his image.'

'I have purpose because God created me, and everyone else, with their own unique personality and abilities.'

All of these are rooted in our Christian beliefs that God is a God of Love, Grace and Faithfulness.

It is the aim of all associated with Cossington Church of England Primary School that all children should have the opportunity to achieve their full potential in all areas of the curriculum and in all other aspects of school life. We promote an ethos in which every stakeholder in the school cares for each other, keeping everyone safe every day. Pupil are taught that they are significant and that everyone has rights and a responsibility to show respect to each other. The school also believes every child has a purpose and an entitlement to achieve to their full potential.

At Cossington Church of England Primary school we aim to work together, guided by our values so we can all grow and flourish academically, spiritually and socially. Through a positive outlook, exploration and excellence we aspire to learn, act and achieve together. The aim of this policy is to ensure the behaviour and attitudes of pupils enables the promotion and success of the above principles and values.

Development, monitoring, and review of this policy This e-safety policy has been developed by a working group made up of: Headteacher Mr Yandell, Deputy Head and E-Safety Co-ordinator Mr McHale and Governors.

Before being finalised, it has been shared and edited with staff, including teachers, support staff and technical staff and has been shared and discussed with governors. It is available to parents to view on the school website. Consultation with the whole school community has taken place through a range of formal and informal meetings. Our e-Safety Policy has been written by the school, building on the Leicesershire LA e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors. The e-Safety Policy and its implementation will be reviewed annually in order to keep up to date with technological advances.

2. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. A member of the Governors has taken on the role of E-safety Governor.

The role of the E-safety Governor will include:

- regular meetings with the E-safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors
- evaluating the effectiveness of E-Safety INSET training.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-safety Co-ordinator.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-safety Coordinator/Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-safety Co-ordinator.
- The Senior Leadership Team will also evaluate the effectiveness of E-Safety INSET training (In school and external)
- If the E-Safety policy is misused, appropriate sanctions and actions will be taken by the Headteacher

E-safety Co-ordinator

The E-safety Coordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, meets regularly with E-safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meeting/committee of Governors
- Reports regularly to Senior Leadership Team
- Manages the schools Social media account in order to promote E-safety on a regular basis
- Provides parents/carers with updates regarding Social Media and E-Safety issues

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- They report any suspected misuse or problem to the Headteacher or E-safety Coordinator for investigation
- All digital communications with pupils/ parents/carers should be on a professional level and only carried out using official school systems

- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- They stay up to date with the latest E-Safety concerns using the Safer Schools application/articles/posters.
- They remain compliant with the Data Protection Law

Pupils

Pupils:

- Are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Have a good understanding of 'Apps', 'Filters' and Photo Editing
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school
- The self-esteem, well being and mental health of our pupils will be a consideration with any of our school policies

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, letters, website, e-safety workshops and campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Their children's personal devices in the school (where this is allowed)
- Parents/Carers must only use images and videos of their child/children for personal use and must not share via social media

3. The importance of safer internet use

- As our students mature, they learn how to recognise difficult situations in many areas. We will help them understand and be safe in the on-line world.
- 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 an essential element in 21st century 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 will need to learn how to evaluate Internet information and to take care of their own safety and security.

4. Educational benefits of the internet

- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- professional development for staff through access to national developments,
- educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support through Primary World
- access to learning wherever and whenever convenient.
- ICT provides access to experts in many fields for pupils and staff;
- access to world-wide educational resources including museums and art galleries;

5. Enhancement of learning through the use of the internet

- The school Internet access will be designed expressly for pupil use and will include 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.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

6. Pupil evaluation of internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

7. Maitenance of information security systems

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media cannot be used to adhere to our strict Data Protection regulations. Staff have the use of secure OneDrive system
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- The Computing Co-ordinator / network manager will review system capacity regularly.
- We employ a Primary World to maintain our school information and security system

8. Management of public 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.
- E-mail addresses should be published carefully, to avoid spam harvesting.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright

9. Pupil's images or work being published

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

- Parents sign consent forms before images of their children are published on the website or elsewhere.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

10. Social networking and personal publishing management

- The schools 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, instant messenger and e-mail addresses, full names of friends, specific interests and clubs etc.
- Teachers must not run social network spaces for student use on a personal basis.
- 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 through Computing lessons to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.

11. Filter management

- If staff or pupils discover unsuitable sites, the URL must be reported to the Computing Co-ordinator.
- 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 CEOP.
- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by Primary World.

12. Management of 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 school should investigate wireless, infra-red and Bluetooth communication technologies and decide a policy on phone use in school.

13. Personal Data protection

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

14. Authorisation of internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access.

15. Assessment of risks

- 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.

16. E-safety complaints procedure

- 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.
- Parents and pupils will need to work in partnership with staff to resolve issues.

17. How is the Internet used 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. How will the policy be introduced to 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.
- There will be parent workshops relating to the issue of e-safety.
- Instruction in responsible and safe use should precede Internet access.
- Every unit of the Computing curriculum has e-safety considerations on the planning, so teachers can build these into their teaching. This will cover both school and home use.
- Children will take part in an e-safety collective worships throughout the school year and Safer Internet Day covering topics such as online footprints; acceptable behaviour and how to report online behaviour.
- The use of our Purple Mash online programme, are taught within the Computing unit. Both services can be used at home.

19. How will the policy be discussed with staff?

- All staff will be given the School e-Safety policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school esafety Policy will be provided as required.

20. Parental support

- Parents' attention will be drawn to the school's e-Safety policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use alongside parent workshops.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to relevant organisations.

21. How will Child Protection be ensured?

- Children and young people may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate or possibly illegal.
- The school has a responsibility to educate pupils and teach them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, particularly social networking sites.
- We will aide parents/carers with this through parent workshops, regular computing events and via the school's official facebook page. Parents will be included as much as possible in this process so

that they can ensure that any access the pupils have to computers and the internet at home is safe.

- Appropriate photographs are taken of children to capture a curriculum activity or a celebration of school life using school equipment but permission will be sought from parents beforehand. Staff will not use their personal mobile phone, camera (still or moving images) or other devices to take, edit or store images of pupils from this school.
- Any concerns will be immediately reported to a DSL.
- Staff will not communicate with pupils through private email accounts, work email accounts, or social networking sites. Staff will be circumspect in their use of social networking sites and will not discuss school business or school issues on their personal social networking site. The school believes it is far safer for staff not to accept either school children or ex-pupils as 'friends'.
- Great care will be taken if staff make an exception to this guidance and will account to the Head teacher for their decision. E.g. young person is also a family member.
- For further information about Child Protection please refer to the Child Protection Policy.

22. Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, school Facebook page etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Reviewed and updated on 27/01/2020
To be reviewed on 27/01/2021

Signed

Headteacher Governor