CAMBO FIRST SCHOOL

e-Safety Policy and Audit

2019

Externally Audited July 2018 - NCC

E-Safety Policy

Policy aims

This online safety policy has been written by Cambo First School involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template.

It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2019, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' 2018 and the local Northumberland Safeguarding Children Multi-agency Partnership procedures.

The purpose of Cambo First School's online safety policy is to

- The Internet is an essential element in 21st century life for education, business and social interaction. Cambo First School has a duty to provide pupils with quality Internet access as part of their learning experience.
- safeguard and promote the welfare of all members of Cambo First School community online.
- identify approaches to educate and raise awareness of online safety throughout our community.
- enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- identify clear procedures to follow when responding to online safety concerns.

Cambo First School identifies that the issues classified within online safety are considerable but can be broadly categorised into three areas of risk.

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users

- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Policy scope

Cambo First School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Cambo First School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.

Cambo First School will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

This policy applies to all staff, including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of Cambo First School as well as learners and parents and carers.

This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

Links with other policies and practices

This policy links with several other policies, practices and action plans, including but not limited to:

- Anti-bullying policy
- Acceptable Use Policies (AUP)
- Code of conduct/staff behaviour policy
- Behaviour policy
- Child protection/safeguarding policy
- Confidentiality policy

- Curriculum policies, such as: ICT, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (SRE)
- Data security
- Cameras and Video use policy
- Mobile phone and social media policies

Monitoring and review

Technology evolves and changes rapidly; as such Cambo First School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.

- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the governing body will be informed of online safety concerns, as appropriate/in termly governing body meetings.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, at termly meetings
- Any issues identified via monitoring policy compliance will be incorporated into an action plan where and when pertinent.

Roles and Responsibilities

The school has an appointed e-Safety Coordinator, [Mrs. P. Cummings]. This person is also the Designated Child Protection Coordinator as the roles overlap. It is recognised that all members of the community have important roles and responsibilities to play with regards to online safety.

We aim to:

- Create a whole setting culture that incorporates online safety throughout all elements of Cambo First School life.

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with technical staff and IT support (Omnicom/NCC) to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

It is the responsibility of all members of staff to:

- Contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the learners in their care.
- Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures.

- Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

It is the responsibility of parents and carers to:

- Read our acceptable use of technology policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement *and* acceptable use of technology policies.
- Seek help and support from the *school* or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as learning platforms and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

Teaching and learning

Why Internet use is important

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

e-Safety in the Curriculum

We will establish and embed a whole *school* culture raising awareness and promoting safe and responsible internet use amongst our learners by:

- ensuring our curriculum and whole *school* approach is developed in line with the UK Council for Internet Safety (UKCIS) '[Education for a Connected World Framework]' and DfE '[Teaching online safety in school]' guidance.

- ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing lessons where pertinent.
- reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
- using external visitors, where appropriate, to complement and support our internal online safety education approaches.
- Cambo First School will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
- displaying acceptable use posters in all rooms with internet access.
- informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
- All classrooms will have an e-safety display.

Cambo First School will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:

- ensuring age appropriate education regarding safe and responsible use precedes internet access.
- supporting learners to evaluate what they see online so they can make effective judgements about if what they see is true, valid or acceptable.
- supporting learners in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
- enabling learners to understand what acceptable and unacceptable online behaviour looks like.
- preparing them to identify possible online risks and make informed decisions about how to act and respond.
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

Vulnerable Learners

Cambo First School recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.

- Cambo First School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
- Staff at Cambo First School will seek input from specialist staff as appropriate, including the Head teacher who is also the DSL, SENCO, Child in Care Designated Teacher to ensure that the policy and curriculum is appropriate to our community's needs.

Managing Internet Access

Filtering and monitoring

www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Cambo First School governors have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.

Our filtering and monitoring software has been purchased via NCC and meets our specific needs and circumstances Sophos/Light Speed. [updated September 19]

Changes to the filtering and monitoring approach will be risk assessed by staff at NCC with educational and technical experience.

The Head teacher will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. [NCC –ICT –SLA]

The governors are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom

management and regular education about safe and responsible use is essential.

Appropriate filtering

Cambo First School's education broadband connectivity is provided through NCC

- Our Software blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
- The provider is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
- The software integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- We work with Northumberland County Council [NCC] to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to turn off the monitor, and report the concern immediately to a member of staff, report the URL of the site to Mrs Cummings who will inform NCC technical services.
- Filtering breaches will be reported to the DSL (or deputy) and technical staff and will be recorded and escalated as appropriate. [Mrs Cummings/Mrs Patterson]
- Parents/carers will be informed of filtering breaches involving learners.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

- monitoring internet and web access (reviewing log file information weekly)
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

If a concern is identified we will:

- respond in line with the child protection policy

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.
- Pupils must not reveal personal details of themselves or others in e-mail
- communication, or arrange to meet anyone without specific permission.
- e-mail 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.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils‟ personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Classroom Use

Cambo First School uses a wide range of technology. This includes access to:

- Computers, laptops, tablets and other digital devices
- Internet, which may include search engines and educational websites

- Learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras

All setting owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.

- All devices are password protected
- All devices have Lightening Speed monitoring software on them
- Filtering software is on all devices.
- Safari is disabled on ipads

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The setting will use appropriate search tools/bookmarked sites as identified following an informed risk assessment.

We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Supervision of internet access and technology use will be appropriate to learners age and ability.

Early Years Foundation Stage and Key Stage 1

- Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

Lower Key Stage 2

- Learners will use age-appropriate search engines and online tools.
- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability

Managing internet access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.
- All staff USB drives are encrypted. Written Records are kept re users

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully
- Pupil's full names will not be used anywhere on the Website or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for first school aged pupils.

Managing filtering

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it 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.

Managing video conferencing [should the need arise]

- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils" age.

Reducing On Line Risks

Cambo First School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will

- regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use in the school is permitted.
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.

- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence. This is clearly outlined in our acceptable use of technology policies and highlighted through a variety of education and training approaches.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998/ GDPR 2018.

Handling e-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 Headteacher.
- 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.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

Introducing the e-Safety Policy to pupils

- e-Safety Rules will be posted in all classrooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety Policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Enlisting parents' support
- Parents" attention will be drawn to the School e-Safety Policy in annual e-safety briefings, newsletters, the school prospectus and on the school website.

This policy was written and agreed by staff. The Policy was formulated after considering the following: aims and content; teaching strategies; dissemination and consultation process.

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an e-Safety Policy that complies with CFE guidance?	Y
The Policy was agreed by governors on: Autumn 2019 [ratified Autumn 19 reviewed annually]	
The Policy is available for staff in: the school office. A copy for new staff is also present in the school staff handbook given on entry to school also on the school website	
And for parents in: the school office and on the school website	
The Designated Child Protection Coordinator is: Mrs Paula Cummings [head teacher] In her absence Mrs Patterson is also a Designated Child Protection Person	
The e-Safety Coordinator is: Mrs. Paula Cummings [headteacher]	
Has e-safety training been provided for both students and staff?	Y 2019John Devlin
Do all staff sign an ICT Code of Conduct on appointment?	Y
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y
Have school e-Safety Rules been set for students?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access [NCC]	Y
Has an ICT security audit been initiated by SMT, possibly using external expertise? [Omnicom] [NCC 2018-19]	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act/GDPR?	Y

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. keep bookmarks Web quest UK School 360
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Ask Jeeves for kids - Yahooligans - CBBC Search - Kids click
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM EasyMail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries School 360
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Kent Grid for Learning Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learning grids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Use of chat rooms in school is forbidden Sites blocked Pupils should never give out personal information.	SuperClubs Skype Flash Meeting Face book etc
Audio and video conferencing to gather information and share pupils' work.	No facilities in school Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype Flash Meeting National Archives "On-Line" Global Leap Natural History Museum Imperial War Museum

Appendix 2 staff code of conduct

Staff Information Systems Code of Conduct

September 2019

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 students 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: …… Capitals: …… Date: ……

Accepted for school: …….. Capitals: ……

Appendix 3

Cambo First School e-Safety Consent Form

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Our School
e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:	***Form:***

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names unless in the newspaper or press reports.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet using a user name and password. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Please complete, sign and return to Mrs. Flatman, the school secretary

Reception/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.

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.