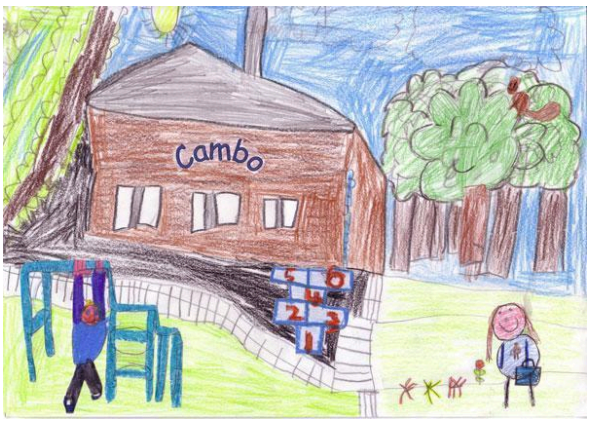
CAMBO FIRST SCHOOL

e-Safety Policy and Audit

2024-25

Externally Audited Summer 2021 - NCC



Cambo First School

Online E-Safety Policy

Date policy last reviewed: Oct 24

Signed by:

P Cummings 18/10/24

Headteacher Date:

PAV Walker November 24

Chair of governors Date:

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Child-on-child sexual abuse and harassment
6. Grooming and exploitation
7. Mental health
8. Online hoaxes and harmful online challenges
9. Cyber-crime
10. Online safety training for staff
11. Online safety and the curriculum
12. Use of technology in the classroom
13. Use of smart technology
14. Educating parents
15. Internet access
16. Filtering and monitoring online activity
17. Network security
18. Emails
19. Social networking
20. The school website
21. Use of devices
22. Remote learning
23. Monitoring and review

Appendix

A. Online harms and risks – curriculum coverage

Statement of intent

Cambo First School understands that using online services is an important aspect of raising educational standards, promoting child achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of children and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect children and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all children and staff.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) Filtering and monitoring standards for schools and colleges
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DFE [2023] 'Working together to keep children safe 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Childs' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Remote Education Policy

2. Roles and responsibilities

The governing body will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.

- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed
- Ensuring staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher/DSL will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping children safe.
- Working with staff and the governing board to update this policy on an annual basis.

The Headteacher/DSL will also be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that children with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the ICT technician.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by children and staff, and ensuring all members of the school community understand this procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.

- understanding the filtering and monitoring processes in place at the school.

- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school

ICT technician will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members will be responsible for:

- Contributing to the development of our online safety policies.
- Reading and adhering to our online safety policy and acceptable use of technology policies.
- The security of IT systems and the electronic data they use or have access to.
- Modelling good practice when using technology with learners
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Embedding online safety education in curriculum delivery wherever possible.
- Having an awareness of a range of online safety issues and how they may be experienced by the learners in their care.
- Identifying online safety concerns and taking appropriate action by following the school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, including reporting to the HT/DSL and signposting learners and parents/carers to appropriate support, internally and externally.
- Taking personal responsibility for professional development in this area.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that children may be unsafe online.

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
- Reporting online safety incidents and concerns in line with the procedures within this policy.

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.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The HT/DSL has overall responsibility for the school's approach to online safety, with support from Staff where appropriate, and will ensure that there are strong processes in place to handle any concerns about children's' safety online. The HT/DSL will liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by childs to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that children displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis

whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a child's online behaviour are reported to the HT/DSL, who investigates concerns with relevant staff members, e.g. ICT technician, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising childrens, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a child has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain children can be more at risk of abuse and/or bullying online, such as LGBTQ+ children and children with SEND.

Cyberbullying against children or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

5. Child-on-child sexual abuse and harassment

Childs may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that children are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to children becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other children taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that children who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the child may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact children are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The HT/DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a child may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about children with relation to CSE or CCE, they will bring these concerns to the HT/DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain children at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any children displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a child relating to radicalisation, they will report this to the HT/DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a child's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites

and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a child is suffering from challenges in their mental health. Concerns about the mental health of a child will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the child and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst children in the school, they will report this to the HT/DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to children, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the HT/DSL and the will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing children.
- Not inadvertently encouraging children to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger children but is almost exclusively being shared amongst older children.
- Proportional to the actual or perceived risk.
- Helpful to the children who are, or are perceived to be, at risk.
- Appropriate for the relevant child's' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the HT/DSL's assessment finds an online challenge to be putting children at risk of harm, they will ensure that the challenge is directly addressed to the relevant children, e.g. those within a particular age range that is directly affected or individual childfdn at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing childrens' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that childs with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a child's use of technology and their intentions with regard to using their skill and affinity towards it, the HT/DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The HT/DSL will ensure that childREN are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The HT/DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation.

; and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that children are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and health education
- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to children's ages and developmental stages.

Children are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app

they are using. The underpinning knowledge and behaviours children learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks children may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix A of this policy.

The HT/DSL will be involved with the development of the school's online safety curriculum. Children will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, will work together to ensure the curriculum is tailored so that children who may be more vulnerable to online harms, e.g. children with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from children.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of children.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher/DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

The class teacher and HT/DSL, where pertinent, will consider the topic that is being covered and the potential that child in the class have suffered or may be suffering from online abuse or harm in this way. The HT/DSL will advise the staff member on how to best support any child who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a child who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which children feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything children raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a child makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Ipads
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that children use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Children will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Children will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Children.

Staff will use all smart technology and personal technology in line with the school's Staff ICT and Electronic Devices Policy.

The school recognises that childrens' unlimited and unrestricted access to the internet via mobile phone networks means that some children may use the internet in a way which breaches the school's acceptable use of ICT agreement for children.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Children will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban child's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among children, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating children about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

The school will work in partnership with parents to ensure children stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of childs, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- NOS – Wake Up Wednesday
- Website
- Newsletters
- Online resources

15. Internet access

Children, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and

monitoring to ensure individuals are using the internet appropriately. [being rural it is nigh on impossible to access mobile networks from school]

16. Filtering and monitoring online activity

www.saferinternet.org.uk/advice-centre/teachers-and-schoolstaff/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/Bit Defender. [updated September 23]

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.

All members of staff have their own unique usernames and private passwords to access the school systems

Pupils have their own unique user names and password to access the school systems.

Mrs Cummings, reviews filtering software messages on Monday mornings and takes any actions deemed necessary.

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 HT/DSL/Deputy DSL and technical staff and will be recorded and escalated as appropriate. [Mrs Cummings/Mrs Patterson/ NCC -Allan Smith]

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.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the HT/DSL and ICT technician, who will escalate the matter appropriately. If a child has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the HT/DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by the NCC ICT technician.[SLA] Firewalls will be switched on at all times. The ICT technician will review the firewalls on a monthly basis to ensure they are running correctly, and to carry out any required updates.

Staff and children will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to the HT/DSL who will inform NCC and NCC ICT technician.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Children in class 2, will be provided with their own unique username and private passwords. Staff members and children will be responsible for keeping their passwords private..

Users will inform the HT/DSL and NCC ICT technician if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to log out/ lock access to devices and systems when they are not in use.

Full details of the school's network security measures can be found in the Cyber-security Policy.

18. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Child Confidentiality Policy and Staff and Volunteer Confidentiality Policy.

Staff will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to the HT/DSL or ICT technician. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

e-mail

• Children may only use approved e-mail accounts on the school system.

• Children must immediately tell a teacher if they receive offensive email.

• Children 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 website

• The contact details on the Website should be the school address, e-mail and telephone number. Staff or children‟ 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 Sophos/Bid defender monitoring software on them

• Filtering/Virus protection 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 [rarely used now]

Publishing children's images and work

Photographs that include children will be selected carefully

Children'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 children are published on the school Website.

Children's work can only be published with the permission of the child 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.

Children will be advised never to give out personal details of any kind which may identify them or their location.

Children and parents will be advised that the use of social network spaces outside school is inappropriate for first school aged children.

Managing filtering

The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect children are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the HT/DSL

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.

Children should ask permission from the supervising teacher before making or answering a video conference call.

Videoconferencing will be appropriately supervised for the child's age.

Reducing Online 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 children

e-Safety Rules will be posted in all classrooms and discussed with the pupils at the start of each year.

Children 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.

School Owned Devices

Staff members and child's will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement.

19. Remote learning

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

20. Monitoring and review

This policy will be reviewed annually. The next scheduled review date for this policy is October 2023. Any changes made to this policy are communicated to all members of the school community.

Paula Cummings Headteacher  18/10/24
Pamela Walker Chair of Governors P.A.V.Walker Nov 24

E-Safety Audit

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
Date of latest update: May 2008 created /updated Oct 24	
The Policy was agreed by governors on: Autumn 2008 [ratified Nov 24 reviewed annually]	
The Policy is available for staff in: the school office/on the school website. A copy for new staff is also present in the school staff handbook given on entry to school	
And for parents in: the school office/website	
The DSL Coordinator is: Mrs Paula Cummings [head teacher] Deputy DSL Mrs Elizabeth Patterson. Governor for Safeguarding is Isobel Anderson/Pamela Walker	
The e-Safety Coordinator is: Mrs. Paula Cummings [headteacher]	
Has e-safety training been provided for both children and staff? Via National Online Safety. School subscription annually.	Y
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? Reception/new to school	Y
Have school e-Safety Rules been set for children?	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 SLA]	Y
Has an ICT security audit been initiated by SMT, possibly using external expertise?	Y

Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

Appendix 1: Internet use - Possible teaching and learning activities

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 Northumberland Grid for Learning
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. • 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.school 360	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

Online harms and risks – curriculum coverage

Reception to Y4 . We do not have upper KS2

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following: ● That age verification exists and why some online platforms ask users to verify their age ● Why age restrictions exist ● That content that requires age verification can be damaging to under-age consumers ● What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm will be covered in the following curriculum areas: ● Health education ● Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include the following: ● What a digital footprint is, how it develops and how it can affect a child's futures ● How cookies work ● How content can be shared, tagged and traced ● How difficult it is to remove something once it has been shared online ● What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm will be covered in the following curriculum areas: ● Relationships education

Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: ● Disinformation and why individuals or groups choose to share false information in order to deliberately deceive ● Misinformation and being aware that false and misleading information can be shared inadvertently ● Malinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs ● Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons ● That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online ● How to measure and check authenticity online ● The potential consequences of sharing information that may not be true	This risk or harm will be covered in the following curriculum areas: ● Relationships and health education ● Computing
[Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following: ● How to recognise fake URLs and websites ● What secure markings on websites are and how to assess the sources of emails ● The risks of entering information to a website which is not secure ● What children should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email ● Who children should go to for support ● The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	This risk or harm will be covered in the following curriculum areas: ● Relationships education ●

Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: ● What identity fraud, scams and phishing are ● That online fraud can be highly sophisticated and that anyone can be a victim ● How to protect yourself and others against different types of online fraud ● How to identify 'money mule' schemes and recruiters ● The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal ● The risk of sharing personal information that could be used by fraudsters ● That children are sometimes targeted to access adults' data ● What 'good' companies will and will not do when it comes to personal details ● How to report fraud, phishing attempts, suspicious websites and adverts	This risk or harm will be covered in the following curriculum areas: ● Relationships education ● Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following: ● Why passwords are important, how to keep them safe and that others might try to get people to reveal them ● How to recognise phishing scams ● The importance of online security to protect against viruses that are designed to gain access to password information ● What to do when a password is compromised or thought to be compromised	This risk or harm will be covered in the following curriculum areas: ● Relationships education ●
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following: ● How cookies work ● How data is farmed from sources which look neutral	This risk or harm will be covered in the following curriculum areas: ● Relationships education ●

	● How and why personal data is shared by online companies ● How children can protect themselves and that acting quickly is essential when something happens ● The rights children have with regards to their data ● How to limit the data companies can gather	●
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following: ● That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue ● How notifications are used to pull users back online	This risk or harm will be covered in the following curriculum areas: ● Health education ● Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following: ● How to find information about privacy settings on various sites, apps, devices and platforms ● That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: ● Relationships education ●
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include the following: ● How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts ● How the targeting is done ● The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm will be covered in the following curriculum areas: ● Relationships education ●
How to stay safe online		

Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following: ● The types of online abuse, including sexual harassment, bullying, trolling and intimidation ● When online abuse can become illegal ● How to respond to online abuse and how to access support ● How to respond when the abuse is anonymous ● The potential implications of online abuse ● What acceptable and unacceptable online behaviours look like	This risk or harm will be covered in the following curriculum areas: ● Relationships education ●
Radicalisation	Childs are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: ● How to recognise extremist behaviour and content online ● Which actions could be identified as criminal activity ● Techniques used for persuasion ● How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following: ● What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal ● How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why ● That it is okay to say no and to not take part in a challenge ● How and where to go for help ● The importance of telling an adult about challenges which include threats or secrecy, such as ‘chain letter’ style challenges	This risk or harm will be covered in the following curriculum areas: ● Relationships education ●

Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following: ● That online content (sometimes gang related) can glamorise the possession of weapons and drugs ● That to intentionally encourage or assist in an offence is also a criminal offence ● How and where to get help if they are worried about involvement in violence	This risk or harm will be covered in the following curriculum areas: ● Relationships education
Fake profiles	Not everyone online is who they say they are. Teaching will include the following: ● That, in some cases, profiles may be people posing as someone they are not or may be 'bots' ● How to look out for fake profiles	This risk or harm will be covered in the following curriculum areas: ● Relationships education ●
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following: ● Boundaries in friendships with peers, in families, and with others ● Key indicators of grooming behaviour ● The importance of disengaging from contact with suspected grooming and telling a trusted adult ● How and where to report grooming both in school and to the police At all stages, it is important to balance teaching childs about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm will be covered in the following curriculum areas: ● Relationships education ●
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

	• That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people children do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	• Relationships education •
Wellbeing		
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following: • How to evaluate critically what children are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for children to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect children and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm will be covered in the following curriculum areas: • Health education
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

	● How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	● Relationships education ●
Suicide, self-harm and eating disorders	Childs may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for children and should take care to avoid giving instructions or methods and avoid using language, videos and images.	

21. ***Staff Information Systems Code of Conduct***

22. ***September 2024***

23. ***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 eSafety 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

24. *Cambo First School*

25. *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.