Cumnor C E Primary School

E-Safety & Anti-cyberbullying Policy

Agreed by Governors:

April 2017

Vorrey Carr (Chair of Govs)

Ed Read (Headteacher)

1. Our Vision

We are living in an increasingly connected world where, alongside the benefits of access to technology, come increased risks to children. Lack of guidance and learning in E-safety can mean children are unaware of the unintended consequences of their on-line behaviour or actions. It highlights the need to educate pupils and the school community about the benefits and risks of using Internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to control their online experience.

'Our vision is to make the children at Cumnor School as safe and productive in the on-line world, both in school and outside of school, as they are in the real world with particular focus on protection against grooming, cyberbullying and becoming a positive e-citizen.'

Our policy and practice against this is clearly articulated in this E-Safety Policy.

2. What is E-safety?

E-safety is a school's ability to protect and educate a school's pupils and staff in their use of technology as well as having appropriate mechanisms in place to respond to, and support any incident where appropriate.

a. Protect

Protecting pupils means providing a safe learning environment by using appropriate monitoring and filtering to control what children can access while at school. But, this only protects them while they are on school premises. Education around e-safety is the only way to ensure that, wherever they are, they know how to stay safe online.

b. Educate

Learning about e-safety is a vital life skill. Empowering children at an early age with the knowledge to safeguard themselves and their personal information is something that needs to be nurtured throughout school to see them into adult life. Equally it is important to empower adults, particularly parents, with the right information so that they can identify risky behaviour, or mitigate the possibility of risk.

The School's E-safety curriculum is progressive and covers a wide range of aspects, including:

- Online behaviour – understanding what constitutes cyber-bullying, inappropriate content and sexting, how to behave safely and with respect for others.
- Protecting your online reputation – understanding both the risks and rewards of sharing personal information online (your digital footprint).
- Learning to evaluate internet content – understanding how to research, evaluate and use published material

c. Respond

Responding to issues is both about ensuring pupils know what to do if anything happens to put their online safety at risk, and taking direct and immediate action as a school where incidents occur.

Cumnor CE Primary School has clear and robust policies and procedures to identify and immediately respond to e-safety risks or incidents, efficiently and consistently. It is important to note that the school's remit to act goes beyond the classroom, to regulate pupils' conduct and safeguard them when they are not on school premises or under the lawful charge of school staff.

3. Why use the internet for Teaching and Learning?

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the internet.

The rapid developments in electronic communications are having many effects on society. Only ten years ago we were asking whether the Internet should be used in all schools. Now, it is an essential aspect of learning across all walks of life. In school, access to the internet is essential to:

- Raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions.
- Prepare children and young people for life in 21st century in terms of education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Teach pupils how to evaluate internet information and to take care of their own safety and security rather than be sheltered from potential risks.

There are many benefits of the Internet to learning:

- Access to world-wide educational resources
- Collaboration and communication between pupils
- Access to anytime, anywhere learning
- Educational and cultural exchanges between pupils world-wide to develop global understanding
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and example of effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of information

With increased use of the Internet, protecting and educating pupils to manage the risk becomes our primary concern. As a school we commit to provide parents with support and information in keeping children safe online.

4. Who does this policy cover?

There are multiple groups that are impacted by this Policy. They are:

- Pupils
- Staff
- Parents
- School Governing Body

a. Pupils

A pupil's perceptions of risks will vary; the school has a clear 'Acceptable Use Policy'. To support appropriate access to the Internet and use of electronic communications, we ensure that:

- The Acceptable Use Policy is shared with pupils, and parents are encouraged to discuss and emphasise the policy for home use.
- Pupils are frequently informed that internet use is monitored.
- A professionally led E-safety training programme is delivered to all pupils to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools. This programme is delivered in the classroom through computing skills lessons and PSHE sessions, and beyond the classroom through structured annual training and specially focused assemblies. E-safety messages are re-enforced each time Internet access or ICT usage is given.

b. Staff and Volunteers

Cumnor CE Primary School's e-safety policy will only be effective if all staff, and support volunteers subscribe to its values and methods. As standard practice we ensure that:

- All members of staff are given the school e-safety policy and its application and importance explained.
- Members of staff are fully aware that Internet traffic can and will be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The e-safety & acceptable use policies are a core part of the induction programme for any new staff and volunteers.
- Training for teaching and non-teaching staff in safe and responsible Internet use and on the school e-safety policy is provided regularly.

c. Parents

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unintended unrestricted access to the Internet. As a school, we recognise the importance of striking a careful balance between informing and alarming parents. Our policy is to:

- Draw parents' attention to e-safety resources, in particular the school's E-safety Policy, relevant articles and resources from trusted sources, and online reporting procedures in newsletters and on the school website.
- Handle internet issues sensitively, to inform parents without alarm.
- Encourage a partnership approach with parents where careful and informed practice can be supported in and out of school. This includes professionally delivered parent e-safety information evenings that build awareness of benefits and risks, and offer independent advice and best practice suggestions for safe home Internet and e-communications use.

d. School Governing Body

All Governors of the school are expected to understand, uphold and ensure e-safety best practice for staff and pupils. As internet and communications access broadens, so governors must ensure that the school keeps pace in its policies and procedures, and can effectively protect, educate and respond.

5. Policy

a. Cyber Bullying

Online bullying and harassment via instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and unintended involvement an increased risk. Cumnor CE Primary School has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.

These include:

- No access to public chat-rooms, instant messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources. Specific education and training on cyber bullying (understanding what behaviour constitutes cyberbullying and its impact,

how to handle concerns and report incidents) is given as part of an annual anti-bullying week and e-safety day.

- Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with staff, who have a range of materials available to support pupils and their families.
- Pupils are informed on how to report cyber bullying both directly within the platform they are on, and to school.
- Complaints of cyber bullying are dealt with in accordance with our anti-bullying policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

b. Grooming

Grooming is a word used to describe how people who want to co-opt or potentially harm children and young people get close to them, and often their families, and gain their trust. Online grooming may occur by people forming relationships with children and pretending to be their friend. They do this by finding out information and seeking to establish false trust. The school has measures in place to educate and protect pupils against this risk. These include:

- No access to public chat-rooms, instant messaging services and bulletin boards.
- No mobile phones.
- All online access and pupil generated content in school is monitored and password protected.
- Pupils are taught how to behave responsibly on line and the 'golden rules' in protecting personal information. More information is outlined in Section 7 of this Policy: Behaviours.
- Pupils, staff, parents and governors are provided with appropriately targeted training on risks and solutions to keep safe on line.

c. School Managed Content and Authorised Access

Cumnor CE Primary School has very clear measures and controls in place to enable responsible internet access and usage. These are outlined as a key part of this e-safety policy, as below:

Authorising Internet Use:

At Cumnor CE Primary School pupil usage is supervised, with access to specific, approved online materials. Pupils are authorised to access the internet as a group or independently, depending on the activity. All staff must read the 'Staff Acceptable Use Policy' before using any school ICT resource.

Managing Filtering:

Whilst levels of internet access and supervision will vary according to the pupils' age and experience, our policy is that internet access must be appropriate for all members of the school community. Our Internet connection was arranged by IT support company 123 ICT following advice from Oxfordshire County Council. Our Broadband is received by a dedicated Internet connection and is tailored with filters to our specific needs. The procedures for ongoing management and review are:

- The school will work with 123 ICT to ensure that systems are reviewed and any improvements are implemented.
- If staff or pupils discover unsuitable sites, the URL must be reported to a member of the 123ICT team who will then ensure that the URL is blocked.
- Any material that the school believes to be illegal must be reported to appropriate agencies (IWF or CEOP)

Managing E-mail and Communications:

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits.

All members of staff are given a secure school e-mail address upon joining the school. The creation of these accounts is the responsibility of the school's business manager. Should any staff need to contact parents directly then they should use their school e-mail, or if relevant, the school mobile,

otherwise all communications should be passed on by the school office. All personal contact details for staff members will remain private.

Pupils have individual e-mail accounts which are ring fenced so that they can only contact staff and children within school. Pupils are made aware that e-mails are monitored and that misuse may lead to suspension of their account.

Password Protection:

Upon joining the school, the system administrator creates a unique username and generic password for each child that they can use to log into the school's network. As part of computing lessons and E-safety teaching, children are taught about the importance of keeping their personal details, including passwords, private.

Managing Published Content and Images:

Our school website celebrates pupils' work, promotes the school, publishes resources and acts as a communication tool. Publication of information on the Cumnor CE Primary School website is carefully considered from a personal and school security viewpoint.

Contact details available on the website are school address, e-mail and telephone number. Staff or pupils' personal information must not be published and all images used will comply with the conditions below:

- Children's names are not published on the website.
- Any images of children must not be labelled with their names.
- Children will only be shown in photos where they are suitably dressed.
- Completed consent forms from parents or carers must be obtained before images of pupils are electronically published.
- A master list is available and updated by the school office staff.
- While images may be taken by parents, it is requested that they are not shared in the public domain.
- All digital images are securely stored and disposed of in accordance with the Data Protection Act.

Managing Information Services:

Cumnor CE Primary School commit to take due care in regard to managing the provision of Information Services to support secure and appropriate access. The measures outlined in this Policy include:

- Network servers are kept securely in a locked room.
- The security of the school information system is reviewed regularly.
- The school keeps the network secure with a number of group policy settings and permissions which only allow certain users to use portable storage devices and to access and open certain drives and files.
- The school reserves the right to monitor user areas and equipment provided by the school.
- Sophos anti-virus software updates automatically
- The school uses Internet firewall and filters
- For fire safety network server backups of user data are taken daily and stored remotely using online servers.

d. Social Networking and Personal Publishing

Parents and teachers need to be aware that the internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. There is increasing educational potential of such tools, for example in the use of blogs and wikis to improve writing.

However, whilst direct access to social networking sites in school is limited and regulated, a significant number of pupils in upper KS2 now use social networking out of school hours on a regular

basis. As a school, we recognise that they may need guidance and support in knowing how to stay safe in such sites, and parents may not know what advice to give them. Pupils need to be encouraged to consider the implications of uploading personal information and the relative ease of adding the information and the practical impossibility of removing it.

Pupils need to be taught the reasons for caution in publishing personal information and photographs on the Internet and in particular on social networking sites. Our e-safety policy aims to provide guidance and council on keeping safe within social networking and personal publishing. Specific council is:

- Within school hours, the school blocks access to social networking sites unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind, which may identify them or their location.
- Examples would include real name, address, mobile or landline phone numbers, school attended,
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Staff must ensure their profiles on social networking sites are private and not to add past or present pupils as friends.
- Staff should not give out their personal email address to parents. All communications must go through the school office.
- Staff and pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others. They are advised not to publish specific and detailed private thoughts.

We very much acknowledge that we cannot act in isolation and parent co-operation in supporting these steps is greatly appreciated.

e. E-Safety Complaints

For safe practice to be a reality, pupils, teachers and parents must know how to submit a complaint. The Complaints Policy is available on the school website and in paper form from the school office.

f. Risk Assessments

In-line with commitments made within this policy, the school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never appear on a school computer. All Internet access at Cumnor CE Primary School is filtered through the LA filtering system. Whilst very robust in their practices around internet use, neither the school, 123 ICT nor Schools Broadband can accept liability for the material accessed, or any consequences resulting from Internet use.

In order to ensure that risk is minimised, the following actions are taken:

- Methods to identify, assess and minimise risks are reviewed regularly.
- Staff, parents, governors and advisers work to establish agreement that every reasonable measure is being taken.
- Pupils are taught to consider the risks of using the internet and how best to manage them.
- The Head teacher will ensure that the e-safety Policy is implemented and compliance with the Policy monitored.

6. Guidelines by Technology

The Policy is applied across a range of technologies that continue to expand and evolve. In addition to computers and tablet devises commonly used to access the Internet or enable communications, this Policy outlines clear guidelines as they apply to other known and used technologies. Specifically:

a. Video Conferencing

Video conferencing, including Skype and FaceTime, enables users to see and hear each other between different locations. It is a 'real time' interactive technology and has many uses in education. The practices below aim to ensure that we apply our e-safety commitments to video conferencing.

Equipment:

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- IP video conferencing must use the educational broadband network to ensure quality of service and security rather than the Internet.
- Video conferencing contact information will not be put on the school website
- The equipment must be secure and locked away when not in use.

Users:

- Video conferencing will be supervised by an appropriate adult at all times.
- Pupils must ask permission from the teacher before making or answering a video conference call.

Content:

When a lesson is to be recorded, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of video conference must be clear to all parties at the start of the conference. The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, checks will be made to ensure that they are delivering material that is appropriate for the audience.

b. Internet enabled mobile phones and handheld devices

Increasingly, a greater number of young people have access to new and sophisticated Internet-enabled devices such as SMART mobile phones, tablets and music players. It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Our policy is that pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

However, in acknowledgement of the growing use, pupils will be taught about the benefits and risks, the legal and moral implications of posting photos and personal information from mobile phones to public websites, and how the data protection and privacy laws apply.

c. Online Gaming

Online gaming can be a helpful and engaging way of developing learning through play with a range of educational content presented through games to support literacy, maths, problem solving, strategy or coding. Controlled use may be supported within the classroom but always through screened individual log-in programs or via teacher lead activity where fit for use and appropriate access settings have been pre-assessed.

However, we also recognise that gaming plays a key part in recreational play in the home setting or when with friends. We have therefore outlined some best practice guidance from Microsoft which will help to support and keep children safe when gaming online.

Making safe choices:

All games have age guidance ratings so that content can be assessed as appropriate. Check the ratings of the games your children want to play. In the UK most games for consoles or online have a PEGI rating which can be found on pack or searched for via the PEGI website. You can use these ratings as you discuss the most appropriate games with your child

Beyond the content rating, selecting games that are well-known or those from reputable sites will reduce the risk of downloading viruses or sharing data in an unprotected way. You can also review the game's terms of play to find out how the game service monitors players and responds to abuse and read the site's privacy policy to learn how it will use and protect children's information.
Games that have no on-line connection, no entry of personal data or passwords and that are user only controlled do not pose a potential e-safety risk, however, to add an extra dimension to a game there is increasingly a multiplayer element, where players often communicate via integrated chat or verbally with microphone or a headset.
Many games – from simple chess to first-person adventure games, where thousands of players participate simultaneously – include these features. The presence of such a large online community of anonymous strangers and the unfiltered, unmoderated discussions, can pose a variety of potential risks such as:

- Inadvertently giving away personal information, including password, email or home address or age.
- Inappropriate contact or behaviour from other gamers
- Buying or selling virtual, in-game property – for example high-level characters – where there is real money involved.
- Disposing of game consoles, PCs and mobile devices without deleting your personal information and account details.
- Playing games for many hours at a time with the danger of becoming addicted.

Recommended solutions:

Gaming can be an enriching learning experience with some simple steps to keep safe:

- Play online games only when you have effective and updated antivirus software and firewall running.
- Play only with authorised versions of games which you have purchased from the correct sources and for which you have a licence. Verify the authenticity and security of downloaded files and new software by buying from reputable sources.
- Choose a user name and password with your child that does not reveal personal information. Similarly, if the game includes the ability to create a personal profile, or where contact can be made by other players make sure that no personal information is given away.
- Read the manufacturer or hosting company's terms and conditions to make sure there will not be any immediate or future hidden charges.
- When disposing of your gaming device either by selling, scrapping, giving away or donating, ensure all of your persona l information and your account details have been deleted.
- Set guidelines and ground rules for your children when playing online. This could include time limitations, parent entered passwords or game play only in communal areas

7. Behaviour & Sanctions

A critical part of our e-safety policy which applies across all technologies is the behaviour we seek to embed and the sanctions pupils or staff may face if their actions put their or others e-safety at risk.

Pupils' information is personal

Pupils learn to never give out personal details such as name, address, date of birth or school attended.
User names and passwords should not contain personal information

Treat others online as you do in the real world

Pupils learn that online bullying and harassment are potential problems that can have a serious effect on children.

Strangers Online are still strangers

Pupils learn to recognize that friends are people we know and see regularly as part of our everyday lives. Online "friends" are strangers and invitations to meet them in the real world should be reported.

Evaluate what you see and do

Pupils learn to evaluate everything they read, and to refine their own publishing and communications with others via the Internet. They are supported in learning to evaluate internet content.

What to do if something isn't right

Pupils learn that if they know or feel something isn't right that they should speak to, or contact an adult immediately.

Sanctions:

The school would take immediate action if pupils or staff were to put themselves or others at risk. There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.

Pupils: Sanctions within the school behaviour policy will apply:

- Interview/counselling by the headteacher
- Informing, and if appropriate, meeting with parents or carers
- Removal of Internet or computer access for a period.

Staff: As a school we have formally adopted Oxfordshire County Council's Discipline Procedures for all Employees in Schools. It is essential for staff to use the internet, including social media in a responsible and professional manner both in school and out of school, in order to ensure the privacy and safety of all employees, pupils, parents and members of the wider school community.

8. Learning to Evaluate Internet Content

Developing best practice internet use is imperative. Parents and teachers can help pupils learn how to distil the meaning from the mass of information provided on the Internet.

Often the quantity of information is overwhelming and staff guide pupils to appropriate websites, or teach search skills. Information received via the Internet, e-mail, or text message requires good information handling skills. Our approach is to offer younger pupils a few good sites as this is often more effective than an Internet search. Respect for copyright and intellectual property rights, and the correct use of published material are taught.

Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet. Specifically:

- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff members guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity.
- ICT skills lessons are used to educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. This is reinforced by teachers when using the internet within their classroom.
- The school ensures that copying and subsequent use of the Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Anti-Cyberbullying Policy

We aim to ensure that children are safe and feel safe from bullying, harassment and discrimination under the Stay Safe Every Child Matters Agenda. Our school is committed to teaching children the knowledge and skills to be able to use ICT effectively, safely and responsibly.

Cyber bullying Defined:

Cyber bullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.

Aims:

- To ensure that pupils, staff and parents understand what cyber bullying is and how it can be combated.
- To ensure that practices and procedures are agreed to prevent incidents of cyber bullying.
- To ensure that reported incidents of cyber bullying are dealt with effectively and quickly.

Understanding Cyber bullying:

- Cyber bullying is the use of ICT (usually a mobile phone and/or the internet) to abuse another person.
- It can take place anywhere and involve many people.
- Anybody can be targeted including pupils and school staff.
- It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorised publication of private information or images etc.

Procedures to Prevent Cyber bullying:

- Staff, pupils, parents and governors to be made aware of issues surrounding cyber bullying.
- Pupils and parents will be urged to report all incidents of cyber bullying to the school.
- Staff CPD will assist in learning about current technologies.
- Pupils will be involved in developing and communicating this policy.
- Pupils will learn about cyber bullying through PSHE, assemblies, Anti-bullying Week activities and other curriculum projects.
- Pupils will sign an Acceptable Use of ICT Contract.
- Parents will be provided with information and advice on how to combat cyber bullying
- Parents will be expected to sign an Acceptable Use of ICT contract and to discuss its meaning with their children.
- Pupils, parents and staff will be involved in reviewing and revising this policy and school procedure.

All reports of cyber bullying will be investigated, recorded, stored in the Headteacher's office and monitored regularly.The Local Authority can provide support and assistance in dealing with incidents of cyber bullying and can be contacted by staff and parents. The police will be contacted in cases of actual or suspected illegal content.

Appendix 1

Primary Pupil Acceptable Use of ICT Agreement

- I will always treat the school's ICT equipment with care and respect
- I will only use ICT in school for school purposes.
- I will only use my school e-mail address when e-mailing. I will only e-mail teachers and pupils from our school.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will not bring software, CDs or ICT equipment into school without permission.
- I will only use the internet after being given permission from a teacher.
- I will make sure that all ICT contact with other children and adults is safe, responsible and polite.
- I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will tell a teacher immediately.
- I will not give out personal details such as my name, phone number or home address.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my conduct or e-safety.