

COMPUTING & ESAFETY

Including Online Safety and Acceptable Use

Coney Hill Community Primary School



Governor Committee Responsible:	Coney Hill Combined Committee	Staff Lead(s):	Ross Hammond/ SBM
Status <i>(Statutory / Advisory)</i>	Statutory	Review Cycle	Annual
Last Review	November 2024	Next Review Date	November 2025
Headteacher	Dani Brayshaw dbrayshaw@coneyhill.gloucs.sch.uk		
Chair of Governors	Daniel Gillingham chair@chcfederation.gloucs.sch.uk		

Contents

<i>School Vision and Introduction</i>	3
Roles and Responsibilities	4
Managing the school eSafety messages	4
eSafety in the Curriculum	4
Benefits of Internet Access for Education	5
Internet Use in School	5
How pupils will learn to evaluate Internet content	5
How Internet access will be authorised	6
How the risks will be assessed	6
How complaints regarding Internet use will be reported	6
How filtering and monitoring will be managed	6
Internet Publishing Statement	7
Managing Website Content	7
Social Networking and Personal Publishing	7
Managing Emerging Internet Uses	7
Protecting Personal Data	8
Use of Portable Equipment	8
_ Personal Mobile Devices (includes Smart watches)	8
Use of mobile phones by pupils	8
Use of the school mobile phone	9
Use of personal mobiles for work purposes	9
How ICT System Security will be maintained	9
Introducing the Policy to Pupils	9
Staff Consultation and eSafety Staff Training	9
Homeworking remotely for Staff	10
Enlisting Parents' Support	10
Remote Learning	10
Password Security	11
Managing email	11
Webcams	12
Inappropriate material	12
Equal Opportunities	12
Inclusion	12
Pupils with additional needs	12
Monitoring and Review	13
Appendix A Acceptable Use Agreement:	14
Appendix C Acceptable use agreement for pupils bringing mobile phone or smart watches into school	17
Appendix D Permission form allowing a pupil to bring their mobile device to school	18
Appendix E Internet Pupil Acceptable Use	19
Appendix F SMART Rules	20

Our e-Safety Policy has been written with regard to Keeping Children Safe in Education (current version) building on a variety of exemplar policies (with acknowledgement to SWGfL).

School Vision and Introduction

Technology in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Online Safety and Acceptable Use Policy addresses all rights, privileges and responsibilities associated with ICT, computing and the Internet. It encompasses Internet technologies and electronic communications such as mobile phones, as well as collaboration tools and personal publishing. It refers to the safe, acceptable and responsible use of the Internet, highlights the need to educate pupils about the benefits and risks of using technology, and provides safeguards and awareness for users to enable them to control their online experience.

The DSL will take responsibility for online safety and also ensure that there is an appropriate filtering system in place. As stated in KCSiE, the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:-

Content

Contact

Conduct

Commerce

The internet is an essential element in 21st century life for education, business, recreation and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the schools management of information and business administration systems.

At present the school uses Artificial Intelligence for the purposes of improving staff workload and workflow enhancements. Children do not use Artificial Intelligence in their daily learning, but in Year 6 will explore the functions of Artificial Intelligence, its purpose and how to create a training model.

Computing covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of technology within our society as a whole. Currently the technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart technology , including phones - with text, video and/ or web functionality
- Other mobile devices with web functionality

At Coney Hill Community Primary, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both

fixed and mobile internet; technologies provided by the school and technologies owned by pupils and staff, but brought onto school premises.

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Staff, pupils, parents and volunteers sign safe Use of Internet agreements.
- Sound implementation of the Online Safety policy in both administration and curriculum, including secure school network design and use.
- This policy including Online Safety Policy and its implementation will be reviewed annually.
- Safe and secure broadband from the South West Grid for Learning and Gloucestershire Local Authority.
- All Internet access is filtered through a proxy server to screen out undesirable sites at source.
- Informing parents/carers about the School's AUP.

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety lead in our school is Ross Hammond who has been designated this role as part of the computing lead responsibilities. Alongside the computing lead Marie Welch is the school's designated safeguarding lead.

The Filtering and Monitoring Committee meet to share information and update staff appropriately.

All members of the school community have been made aware of who holds this post. It is the role of the eSafety lead to keep abreast of current issues and guidance through maintaining a working knowledge of the responsibilities outlined in Keeping Children Safe in Education and also through the guidance of organisations such as GSCP LA, ICT services for Education, CEOP (Child Exploitation and Online Protection) and Childnet.

The Senior Leadership Team and Governors are updated by the eSafety lead, at times via the Headteacher, and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following school policies: for Behaviour, Anti-Bullying, Data Protection and Security, Freedom of Information, Complaints, Child Protection, Race Equality, Disability Equality Plan, PSHE, CCTV, Remote learning and all other curriculum policies. It was written referencing relevant government guidelines including KCSiE and the Governments ***"Meeting digital and technology standards in schools and colleges"*** guidance

Managing the school eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- A computing display board in school is regularly updated to remind children about staying safe online.

eSafety in the Curriculum

Online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- Internet skills are developed throughout the curriculum and during specific computing sessions.
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.

- Pupils are made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are informed about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

Benefits of Internet Access for Education

- The main reason we provide Internet access to our teachers and pupils is to promote educational excellence by facilitating resource sharing, innovation and communication. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Benefits of using the Internet in education include:

- Access to worldwide educational resources.
- Educational and cultural exchanges between pupils worldwide.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the LA and DCSF.

All Internet users must do so within the boundaries of this policy and failure to do so may result in future internet access being denied.

Internet Use in School

The school will actively take all reasonable precautions to restrict pupil access to both undesirable and illegal material.

- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Rules will be displayed and there will be targeted lessons on Online Safety at the start of each new term.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How pupils will learn to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the DSL.
- The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught, through targeted lessons to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

How Internet access will be authorised

- At Key Stage 1 and Key Stage 2 level, access to the Internet will be by adult demonstration. There will be supervised access to specific websites or to carry out specific web searches; using approved online materials within the normal restrictions of a classroom.

How the risks will be assessed

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Gloucestershire LA can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies recommended by SWGfL will be adopted.
- The Head Teacher will ensure that this policy is implemented and compliance with the policy monitored.

How complaints regarding Internet use will be reported

- Responsibility for handling incidents will be the Headteacher
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.

How filtering and monitoring will be managed

The DSL will take responsibility for online safety and also ensure that there is an appropriate filtering system in place. As stated in KCSiE, the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying,
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- At present the school uses RM Unify/Safety Net (through the Southwest Grid for Learning) for its internet filtering for all internet activity for pupil and staff
- We use Securus for monitoring for all internet activity for pupils and staff
- The school will work in partnership with parents; the Gloucestershire LA, the Department of Education and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported *to the* Internet Service Provider via the DSL.
- The DSL and IT Technician, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Staff training includes understanding roles and responsibilities in relation to filtering and monitoring.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Internet Publishing Statement

The school wishes the school's web site to reflect the diversity of activities, individuals and education that can be found at Coney Hill Community Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles will be adhered to:

- No video recording or photographs will be published without the written consent of the parents/legal guardian of the child concerned (signed on the child's behalf).
- Surnames of children will not be published in conjunction with photographic or video material.
- No link should be made between an individual and any home address.
- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. If in any doubt at all, refer to the DSL.

Managing Website Content

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and only used where parental permission has been given. Pupils' full names will not be associated with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This permission will be sought when the child first joins school and will cover all photographs whilst they are at Coney Hill Community Primary School.
- The Head Teacher will take overall editorial responsibility and ensure content is accurate and appropriate.

Social Networking and Personal Publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing Emerging Internet Uses

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones or smart watches will not be used during lessons or formal school time.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018
- Personal data relating to pupils and staff will only be taken off site if necessary and then encrypted or password protected memory sticks will be used.

Use of Portable Equipment

The school provides portable computing equipment such as laptop computers, and iPads to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

All equipment owned by the school is available for use by all staff. If it is in the care of an individual, access should be negotiated with the individual concerned. Any difficulties should be referred to the Computing lead or IT Technician. All staff are expected to look after any equipment used and report any equipment that is not working properly to the Office. Faulty equipment, laptops or networking problems can also be logged in the 'Support Log' for the IT technician.

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any computing equipment in their care to be returned to school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it.
- If an individual leaves the employment of the school, any computing equipment must be returned.
- The use of USB sticks, re-writeable CDs, etc. to transfer data from external computer systems must be virus free and encrypted.
- No other software may be installed on laptops / devices unless the school owns the licences.

Personal Mobile Devices (includes Smart watches)

See Mobile Phone Policy for more detail

The school allows staff to bring in personal mobile phones and devices for their own personal use.

- Mobile phones must not be used in view of the children unless a member of SLT has agreed permission. Mobile phones must not be used or shared in any way with the children. In emergencies, the school does allow a member of staff to contact a pupil or parent/carer using a mobile device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device and that these devices are not used or shared with the children in any way.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

Use of mobile phones by pupils

- In certain circumstance pupils in year 5 & 6 (exceptional circumstances Year 4) are allowed to bring personal mobile phones to school. These are to be handed into the class teacher at the start of the school day and collected when leaving school.

- Pupils may be allowed to bring in electronic devices for special lessons they will be required to complete a permission form organised by the class staff but the school will accept no responsibility for any loss or damage.

See Appendix C Acceptable use agreement for pupils

Use of the school mobile phone

- Staff are permitted to use the school mobile phone for work purposes and access to the school phone must not be provided to non-staff without authorisation.
- Staff must only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet
- Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line with our staff code of conduct

Use of personal mobiles for work purposes

- In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:
- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits
- Accessing CPOM's two-factor identification codes
- Please refer to the Educational Visits Policy for further guidance on Mobile phones on Educational Visits.

How ICT System Security will be maintained

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Use of data storage devices will be reviewed.
- If being used off site, all information or personal data about the children will be saved onto an encrypted memory stick, which will be provided by the school.
- Personal storage devices may not be brought into school without specific permission and a virus check.
- Files held on the school's network will be regularly checked.
- The IT Technician will ensure that the system has the capacity to take increased Internet use.

Introducing the Policy to Pupils

- Rules for Internet access will be posted near all computer systems.
- Pupils will be informed that Internet use will be monitored. Instruction in responsible and safe use should precede Internet access and online safety will be taught using Project Evolve and SWITCHED ON Computing scheme.
- Other understanding of eSafety instruction/ resources covering both school and home use is included in the Jigsaw online module and Y4 In The Net.

Staff Consultation and eSafety Staff Training

- Staff need to inform the Headteacher of any issues of eSafety that concern them immediately.
- All staff must accept the terms of the 'Acceptable Use Policy' statement before using any Internet resource in school.

- **All** staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Senior management should supervise/oversee the monitoring of Internet use.
- Staff development in the safe and responsible Internet use will be provided as required and will be required to complete online safety training.
- Staff receive termly online safety termly briefing (issued by Knowsley City Learning)
- Rules for responsible use of the Internet will be shared across the school.
- Staff receive regular information and training on eSafety issues in the form of staff updates, school email updates/training from visiting experts and attending appropriate CPD, when available.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
- All teaching staff are expected to incorporate eSafety activities and awareness within their curriculum areas, as appropriate.
- Staff who use You tube in school as a teaching resource are required to sign the unfiltered access agreement (see Appendix B) You tube access is managed by RM unify through SWGFL

Homeworking remotely for Staff

- Homeworking for staff is through RM Unify with 2FA enabled

Enlisting Parents' Support

- Parents' attention will be drawn to this policy in newsletters, and on the school website.
- Classroom communication with parents can be by email.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home. The monthly internet safety newsletter will be communicated to parents.
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
 - Information and celebration evenings
 - Posters/ Notice Boards
 - Website/ Learning Platform postings
 - Newsletter items
 - Emails
 - Parent Texts
 - Parent information evening specifically about online safety by the Police
 - Online safety newsletters subscribed and published by Knowsley City Learning
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Parents/carers of children will be required to sign an acceptable use policy on behalf of the child.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website)

Remote Learning

- All stakeholders to be aware of the requirements of remote learning and how best to Safeguard themselves.

- Pupils and staff will keep passwords safe and adhere to the requirements set out in their specific Acceptable Use Policy.
- All staff ensure they are aware of the requirements set out in the Remote Learning Online Safety Policy 2020.

During times, such as a global pandemic, children may be required to learn remotely from home through the use of our online remote learning platform Showbie and attend live lessons using the video to video conferencing features of Zoom. A separate policy has been created to cover eSafety and Remote learning. This policy is called the Remote Learning Policy 2020 and a copy can be viewed on the school website. In addition, a Remote Learning Risk Assessment for safety control measures and behaviour expectations has been created to further identify and mitigate any associated eSafety risks.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Pupils are not allowed to deliberately access on-line materials or files on the school network of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Computing Lead, IT technician, Business Manager or another member of staff.
- Staff passwords are recommended to be 10 characters long including a capital letter/ a numeric and a special character. Passwords are reset every 90 days.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended in a logged-on state.
- In our school, all computing password policies are the responsibility of the HT and SBM and all staff and pupils are expected to comply with the policies at all times.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- All emails including Governors use 2FA for access to emails
- New staff are given guidance on email use for school business only.
- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. This account must be used for all data relating to the fulfilment of our role as educators. This also includes governors.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Emails which contain personal information should not be sent unless encrypted or password protected.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission. Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the Headteacher if they receive an offensive e-mail.
- It is recommended that all staff emails sent and received are deleted within 1 year of receiving them

Webcams

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, staff training and meetings (mainly through Zoom and Teams).
- Misuse of a webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the headteacher, depending on the seriousness of the offence; investigation by the Headteacher (DSL)/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Equal Opportunities

Coney Hill Community Primary School strives to ensure that the culture and ethos of the school are such that, whatever the heritage and origins, abilities and needs of members of the school community, everyone is equally valued and treats one another with respect. All pupils have the right to be given opportunities and access to the full curriculum regardless of ethnicity, gender, social circumstances, ability, disability, age, nationality or citizenship. Pupils should be provided with the opportunity to experience, understand and celebrate diversity.

Inclusion

The school provides effective learning opportunities for all pupils. When planning, teachers set high expectations and provide opportunities for all pupils to achieve. All teachers are aware that pupils bring to School different experiences, interests and strengths, which will influence the way they learn. Teachers plan their approach to teaching and learning so that all pupils can take part in lessons fully and effectively.

Specific action is taken to enable the effective participation of pupils with disabilities.

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid the establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Monitoring and Review

The governing body are aware of the need to keep this policy up to date, in line with current practice and Government guidance. Therefore, this policy will be monitored and reviewed annually.

Appendix A
Acceptable Use Agreement:
Staff, Governors and Regular Visitors

Agreement / Code of Conduct (September 2024)

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the schools eSafety lead.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteachers or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities, all devices using personnel and/or pupil data must be encrypted.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils except those for whom I am a parent/carer.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteachers or Governing Body.
- I will not install any hardware or software without permission of the Computing Subject Leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images should only be taken on school devices. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will ensure that my online activity (including my use of social media), both in school and outside school, will not bring my professional role, or the school, into disrepute. I will not use social media to discuss school matters which may be in conflict IT with my position.
- I will not use my mobile phone or smart watch in view of the children unless specific permission has been agreed due to exceptional circumstances. For further guidance, please refer to Mobile Phone Policy and the E-Safety policy.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of IT and related technologies.
- I will ensure that any guidance in the current KCSiE (Keeping Children Safe in Education) is followed with regard to Online Safety
- I will ensure that any guidance in the current KCSiE (Keeping Children Safe in Education) is followed with regard to Online Safety and I understand our filtering and monitoring processes on school devices and school networks to keep pupils safe online
- I understand that it is my responsibility to report any Online safety incidences to the Headteacher (DSL) immediately.

Signed agreement _____

Coney Hill Community Primary School

Appendix B Staff Proxy Internet Unfiltered Service Agreement

“You must not leave your browser session open when your computer/ laptop is left either unattended or unlocked “

South West Grid for Learning (SWGfL)

The aim of this agreement is to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk.

The SWGfL encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise the SWGfL's information and computer systems.

The agreement applies to all staff at Coney Hill Community Primary School who use the Staff Proxy Unfiltered Service to assess sites such as You Tube, Facebook, Twitter and any linked sites.

Use of Internet facilities

For the purposes of this agreement, Internet usage means any device with a connection to the Internet via Web browsing, email or newsgroups (public discussion groups) or other software.

Staff Proxy

Unfiltered proxy service is to allow access to certain sites (in which parts may be deemed safe for use as teaching resources but may still not be safe for pupil access) which would normally be blocked. However, this now requires a username and password to access the service which is linked to your computer login and no one else should be given access to your computer login. Passwords are issued on a per user basis and Staff need to keep this password safe and not share with anyone else.

In order to use the Staff Proxy service, you must agree and abide to the Acceptable Use Policy above, and the following conditions in this agreement;

- All internet usage will be logged against your username and that you are subject to the above Acceptable Use Agreement terms and conditions.
- Any inappropriate web access/misuse of this service may cause your access to be revoked and action taken against you.

You must not leave your browser session open when your computer/ laptop is left either unattended or unlocked as unauthorised users (ie. Pupils or Parents may get brief access to this service which would count as misuse and may also cause this service to be revoked from you and or the school.

Therefore you must either close your session of Internet Explorer, or if not you must lock your computer before leaving it unattended.

SWGfL - Monitoring and Access

If inappropriate material is accessed accidentally, staff should immediately report this to the Headteacher Danielle Brayshaw, who will then report to SWGfL, so that this can be taken into account in monitoring.

SWGfL acknowledges that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use (for example investigating racial issues). Any such access should be pre-planned and recorded so that it can be justified if required.

SWGfL will monitor and audit the use of the Internet to see whether users are complying with the agreement. Any potential misuse identified by the SWGfL will be reported to the school.

On evidence provided by the SWGfL, a member of staff may be disciplined by their employer.

At the same time, if a user's conduct and/or action(s) are illegal, the member of staff may become personally liable in some circumstances. Signed agreement _____

Appendix C Acceptable use agreement for pupils bringing mobile phone or smart watches into school

You must obey the following rules if you bring your mobile phone or smart watch to school:

You must not use your mobile phone or smart watch on the school premises.

1. Phones must be switched off (not just put on 'silent').
2. You cannot take photos or recordings (either video or audio) of school staff or other pupils; as per rule on, you should not be using your phone anyway.
3. Avoid sharing your contact details with people you don't know, and don't share other people's contact details without their consent.
4. Don't share your phone's passwords or access codes with anyone else.
5. Don't use your mobile phone to bully, intimidate or harass anyone. This includes bullying, harassing or intimidating pupils or staff via:
 - a. Email
 - b. Text/messaging app
 - c. Social media
6. Don't use your phone to send or receive anything that may be criminal. For instance, by 'sexting'.
7. Rules on bullying, harassment, and intimidation apply to how you use your mobile phone even when you aren't in school.
8. Don't use vulgar, obscene or derogatory language while on the phone or when using social media. This language is not permitted under the school's behaviour policy.
9. Don't use your phone to view or share pornography or other harmful content.
10. You must comply with a request by a member of staff to switch off and hand over, a phone or smart watch. Refusal to comply is a breach of the school's behaviour policy and will be dealt with accordingly.

Pupils are advised that Coney Hill Community Primary School accepts no liability for the loss or damage to mobile phones or smart watches which are brought into school or on to the school grounds.

Pupil agreement

I understand that I am being allowed to use my phone/electrical device during lesson time as part of an educational or class activity.

I will not use my phone or electrical device for any other purpose than the one listed above. If my teacher, or any other member of staff, finds that I am using my phone or electrical device for any other reason, I understand that it will be confiscated.

I understand that the school's Acceptable use agreement for pupils on the use of mobile phones and smart watches still applies.

I understand that Coney Hill Community Primary School accepts no liability for the loss or damage to mobile phones or smart watches which are brought into school or on to the school grounds.

Parent/Carer signature: _____ Class : _____

Appendix D Permission form allowing a pupil to bring their mobile device to school

Use this form to allow pupils to bring their mobile devices to school, for teaching purposes.

It should be signed by parents/carers.

PUPIL DETAILS	
Pupil name:	
Year group/class:	
Parent(s) / Carer(s) name(s):	

The school has agreed to allow the above pupil to bring their mobile device to school of the following reasons.

- For an educational activity during class time

Pupils who bring a mobile phone to school must abide by the school's policy on the use of mobile phones, and its Acceptable use agreement for pupils.

The school reserves the right to revoke permission if pupils don't abide by the policy.

Parents and carers are advised that Coney Hill Community Primary School accepts no liability for the loss or damage to mobile devices which are brought into school or on to the school grounds.

Parent/Carer signature: _____

Appendix E Internet Pupil Acceptable Use

Respect others' opinions and feelings.	
I will: • Use email and discussion to listen to others and understand other peoples' views. • Use polite language.	I will not: • Disrespect other people or gossip about them. • Swear.
Respect others' privacy	
I will: • Keep information about others private. • Only access files that others have given us access to.	I will not: • Discuss or send emails containing information about others that they would not want revealed. • Try to gain access to areas of the internet that are inappropriate.
Protect others and myself	
I will: • Keep my passwords absolutely secret. • Tell a teacher, parent or carer if someone says or does something on the internet that I do not like or makes me unhappy. • Tell a teacher, parent or carer if I find anything inappropriate on the internet. • Follow the internet SMART rules.	I will not: • Allow anyone else to use my username and password under any circumstances. • I will not give other people on the internet my personal information such as my address or telephone number. • I will not use cameras or webcams to give people on the internet photographs of myself. • I will not put photographs or videos of other people onto the internet without their permission.
Keep it legal	
I will: • Make sure anything I do or say on the internet does not harm anybody. • Credit others if I use their ideas or materials.	I will not: Share files such as copyrighted music files or games with others.

Appendix F SMART Rules

There are lots of resources online to help you as well as the following 5 SMART Rules for primary aged children.

Safe:

Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

Meet:

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time

Accepting:

Accepting emails, messages, opening files, images or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable:

Someone online might lie about who they are and information on the internet may not be true. Always check information by looking at other websites, in books, or with someone who knows. If you are going to chat online it's best to only chat to your real world friends and family.

Tell:

Tell a parent, carer or a trusted adult if someone, or something, makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

For more information, take a look at these online resources:

<https://www.childnet.com>

<https://www.thinkuknow.co.uk/parents>

<https://www.nspcc.org.uk/keeping-children-safe/online-safety/#children>

<https://www.saferinternet.org.uk/guide-and-resource/parents-and-carers>