Cogenhoe
Primary School

Online Safety Policy Including Cyber Bullying

	Name	Date
Headteacher's Approval	Charley Oldham	June 2023
Committee Chair's Approval	Gemma Butlin	June 2023
Recommended Review Date:	June 2024 (Annually)	

Version Number
This document is issued and maintained in accordance with Cogenhoe Primary School procedures. Any changes must be clearly identified and discussed with the Governors. The most recent version must be detailed to staff and kept with the other policies for all appropriate stakeholders including parents where applicable.

Version	Date	Description of Change	Changed By
1	September 2015	Implemented & Written	E Noble
2	November 2016	Slight Changes following on-line safety course	E Noble
3	January 2017	Changes as a result of Lesley Pollard Safeguarding Audit	E Noble
4	September 2017	Review	E Noble
5	September 2018	Review – lockers have been provided.	E Noble
6	Jan 2019	Slight review tweaks as a result of LP safeguarding audit	E Noble
7	June 2023	Addition of Smart Watches	R Reeve
8	June 2023	Change of monitoring system to SENSO	R Reeve
9	June 2023	Change wording of e-safety and ICT	R Reeve
10	June 2023	IT support provided by NVP	R Reeve
11	June 2023	Change of names and removal of unnecessary sections	R Reeve

Contents

Writing and reviewing the Online-Safety Policy

- The Online-Safety Policy relates to other policies including those for computing, bullying and for child protection.
- Our Online-Safety Policy has been written by the school, building on the Northamptonshire Online-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

Policy Statement

For clarity, the online-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents

Computing and the internet have become integral to teaching and learning within school, providing children, young people and staff with opportunities to improve understanding and access online resources at the touch of a button.
At present, the internet based technologies children and young people are using inside and outside of the classroom are:

- Websites
- Social Media
- Apps
- Mobile phones
- Other mobile devices such as tablets, smart watches and gaming devices
- Online gaming
- Blogs, Vlogs and Wikis
- Learning Platforms and Virtual Learning Environments
- Email, Instant Messaging and Chat Rooms
- Podcasting
- Video sharing
- Downloading
- On demand TC, video, radio /Smart TVs and live streaming

Technology has many benefits and endless possibilities; however, regardless of one's agenda when using the technologies stated above one thing remains fundamental. This of course being the procedure of appropriate use of internet/technology and the awareness of potential risks alongside age restrictions. As a school and as professionals involved with young children, we must provide a duty of care to protect our pupils and ourselves from harm both within and beyond the school environment. This policy and the procedures implemented are to warrant that every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them.

Organisations must be aware that children and staff cannot be completely prevented from risks using the internet although we can play a part in ensuring the children have the right knowledge and tools to avoid or manage these dangers. In accordance with Ofsted requirements, young people need to be empowered and educated to make healthy and responsible decisions when using the internet – in particular social media. "Technology is not the problem, it is how we use it". Online-Safety, like safeguarding must be a whole school approach, and all staff must take appropriate measures to keep young people and themselves safe using the internet and social media. Members of staff also need to be aware of how to manage their own professional reputation online and demonstrate online behaviours that are in line with their professional role. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children, young people and staff's protection is secure and ongoing.

Online-safety and online safeguarding is situated in an area that is developing at a rapid rate. Therefore to ensure our policy evolves on the same scale, the policy will be due for renewal on an annual basis, or in response to an Online-Safety incident, whichever is sooner. This policy is also to be used in conjunction with the school's Safeguarding Policy and the Staff Handbook.

Both this policy and the Acceptable Use Agreement (for all stakeholders) are inclusive of fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboard, digital video equipment; and technologies owned by pupils and staff, but brought onto school premises (such as mobile phones or other mobile devices).

The aim of this policy is:

- To emphasise the need to educate staff and children about the pros and cons of technology in, and outside of, a school environment
- To provide safeguards and rules for acceptable use to guide the wider school community in their online experiences
- To ensure adults are clear about procedures for misuse of technology within and beyond the school setting.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to the student, or liability to the school.
- To ensure staff are following procedures to educate the children with the knowledge they need in accordance with Ofsted requirements.

The scope of this policy:

This policy applies to all staff, pupils, governors, visitors and contractors accessing the internet or using technological devices on school premises. This includes staff or pupil use of personal devices, such as mobile phones or technologies, which are brought onto school grounds. This policy is also applicable where staff or an individual have been provided with school issued devices for use off-site e.g. a school laptop.

Responsibilities

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy annually, or, in response to any online-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school and to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Online-Safety forms part of the CFC and Curriculum Committees, therefore updates, risk assessments and reviews will be undertaken at these meetings.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for online-safety within our school. The day-to-day management of this will be delegated to a member of staff, the Computing Lead (or more than one), as indicated below.

The Headteacher will ensure that:

- Online-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.

- Online-safety training for staff happens once a year.
- The designated Computing Lead(s) has had appropriate CPD in order to undertake the day to day duties.
- All online-safety incidents are dealt with promptly and appropriately.
- All incidents follow the correct procedure, are logged, filed and necessary staff are informed.

Lead Designated Child Protection Officer

- Remain updated with relevant safeguarding needs regarding online-safety
- Alert and advise the Head and Computing Lead of any necessary additions needed in the policy
- Provide safeguarding training to staff including online - safety procedures and how to respond to online-safety incidents, alongside the Computing Lead.

Computing Lead

The Computing Lead will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/her with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all online-safety matters.
- Engage with parents and the school community on online-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online-safety incident log; ensure staff know what to report and ensure the appropriate audit trail. This is now on the SENSO Cloud.
- Ensure any technical online-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or Computing Technical Support. Otherwise known as Wellbeing and Online Safety Officer.
- Make him/her aware of any reporting function with technical online-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.
- Test filtering software every month to be carried out by Computing Lead and NVP through SENSO/

Computing Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
  - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
  - Any online-safety technical solutions such as Internet filtering are operating correctly.
  - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Computing Lead and Headteacher.
  - That any problems or faults related to filtering are reported to the Safeguarding Officer and the broadband provider immediately, and recorded on the SENSO Cloud or Edukey
  - The SENSO Incident Log is monitored and incidents are reported to the Computing Lead(s).
  - Passwords are applied correctly and regularly changed.
  - He/she keeps up to date with online-safety information in order to maintain the security of the school network.
  - The use of the network by all users is regularly monitored in order that any deliberate of accidental misuse can be reported to the Computing Lead and the Head.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any online safety incident is reported to the Computing Lead (and an EDUKEY Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this online-safety policy are fully understood and a declaration is signed to acknowledge the information, and agree to awareness of the correct procedure should an Online-Safety incident occur.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff must read and sign agreement with the Acceptable Use Policy. This is reviewed every 12 months. This is going to be maintained virtually by NVP
- Personal use of social media sites outside of school is discreet. Advice is given to all staff on this matter. Staff must understand the need to protect their reputations and that of the school, and sign the Acceptable Use Policy to demonstrate this.

All Students

The boundaries of use of equipment and services in this school are given in the student Acceptable Use Policy which is shared with pupils and online rules are displayed around the school. Any deviation or misuse of equipment or services will be dealt with in accordance with the behaviour policy. Online safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school. Online-Safety lessons will be taught as the first lesson of Computing in an academic year and recapped every lesson and more in depth every term.

Through teaching, it will also be made explicit to children that they should speak to an adult immediately.

If staff deal with a disclosure, they must ensure the following points are adhered to, as this will preserve crucial evidence.

- **Screenshot evidence**
- **Never delete any messages**
- **Where possible note the user's name and URL**
- **Inform the Headteacher or Online Safety Lead immediately, who will then contact the police.**

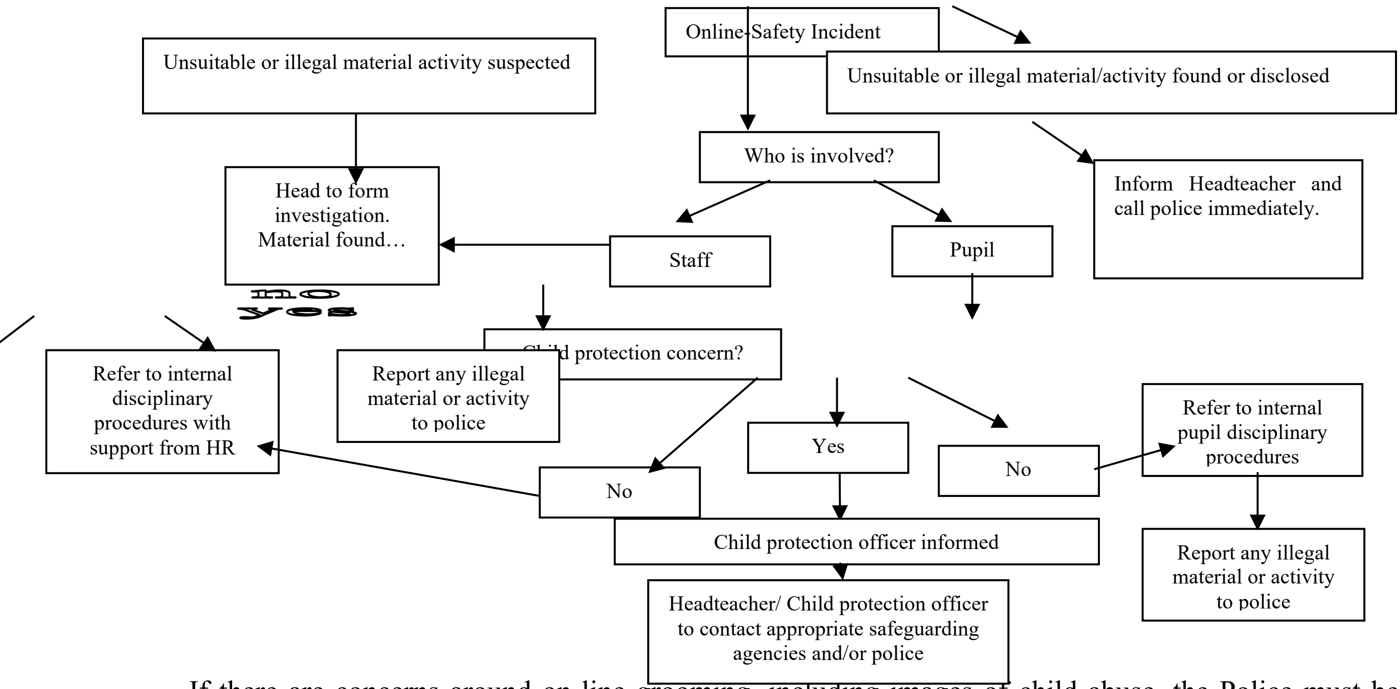
Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. The school will keep parents up to date with new and emerging online-safety risks, and will involve parents in strategies to ensure that students are empowered, yet protected.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will all receive a copy of the student Acceptable Use Policy to read with their children and return signed by the children to emphasise their understanding. We will also be sending out a magazine to all parents 'Digital Parenting' and offering electronic information to support their children with these issues. The school will also be offering a free download of NetAware to familiarise families with recent and current apps e.g. Kik, Snapchat and Oovoo for example. Parent workshops will also be offered by the Online safety lead throughout the academic year. Also signposted to websites such as NSPCC and National Online Safety.

Incident Reporting

In the event of misuse by staff or students, including the use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Head/ Safeguarding Officer immediately, and the Online-Safety flowchart followed. If there is any suspicion that a website may contain child abuse images or any illegal activity, a report should be made to the Police immediately. In the event of minor or accidental misuse, internal investigation would be initiated and disciplinary procedures followed where appropriate.



Online-Safety Incident
Unsuitable or illegal material activity suspected
Unsuitable or illegal material/activity found or disclosed
Who is involved?
Inform Headteacher and call police immediately.
Head to form investigation. Material found…
Staff
Pupil
no
yes
Child protection concern?
Refer to internal disciplinary procedures with support from HR
Report any illegal material or activity to police
Yes
No
No
Refer to internal pupil disciplinary procedures
Report any illegal material or activity to police
Child protection officer informed
Headteacher/ Child protection officer to contact appropriate safeguarding agencies and/or police

If there are concerns around on-line grooming, including images of child abuse, the Police must be contacted immediately. CEOP will also be contacted for extra support. Lessons and workshops for parents will ensure that both children and adults are aware of the role of CEOP and that they can report any incidents at any point.

Other circumstances when online-safety concerns should be reported to the designated safeguarding officer and discussed with the Police are:

- Radicalisation
  - Further information contact Jason.farmer@northants.pnn.police.uk or lscbnorthamptonshire.org.uk/schools/violent…radicalisation
- Hacking
- Hate crimes
- Harassment
- Certain types of adult material
- Criminal conduct, activity or materials

In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches should be reported immediately to the Head and Computing Lead. Details of the procedure are displayed in the staff room.

All incidents must be recorded on EDUKEY to allow for monitoring and auditing. Online-Safety incidents may have an impact on pupils, staff and the wider community both on and off site. These can have legal and disciplinary consequences. Other situations could potentially be very serious and a range of sanctions may be required, which is linked to the school disciplinary policy and child protection policy.

Monitoring

Users are reminded that Internet activity may be monitored at any time without prior notice. This is in order to ensure, as much as possible, that users are not exposed to illegal or inappropriate websites, and to ensure, as much as possible, that users do not actively seek access to illegal or inappropriate websites. Users are made aware of this is the Acceptable Use Policy. All monitoring activities comply with the Data Protection Act 1998, the Human Rights Act 1998, and the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Cyber-Bullying

Cyberbullying is best defined "The use of Information and Communications Technology, particularly mobile phones and the Internet, deliberately to upset someone else". (DCSF 2009)

Despite bullying not being considered a specific criminal act in the UK. There are numerous acts such as the Malicious Communications Act 1998, Protection from Harassment Act 1997, The Public Order Act 1986 and the Communications act 2003 that state harassing or threatening behaviour or communications could be considered a criminal offence. If one of these incidents is committed, assistance will be sought from the Police.

The internet alongside mobile technology is found as a positive, influential and creative part of everyday life. Unfortunately, these technologies are also used in a malicious and negative manner. Young people are often the target of bullying via mobile phones, gaming, social media, apps and chat rooms.

Statistics show:

- **7** in **10** young people are victims of cyberbullying.
- **37%** of them are experiencing cyberbullying on a highly frequent basis.
- **20%** of young people are experiencing extreme cyberbullying on a daily basis.

The saddest statistic of them all is the following:

- 52% of children and young people in England **accept** cyber-bullying as part of everyday life.

This leaves these children with a reduced self-esteem and often results in that young person feeling isolated and alone.

Therefore it is crucial that pupils, staff, parents and carers understand how destructive cyberbullying can be, and how it differs from other forms of bullying. Therefore the school uses assembly, and other online-safety sessions to promote a culture of confident users who know how to address these issues.

Cyber-bullying is extremely likely to take place outside of the school environment; however it will often be reported or disclosed in school. If this incident occurs, it must be acted upon. The DFE guidance on 'Preventing & Tackling Bullying' 2014, states that teachers have the power to discipline pupils for misbehaving outside school premises 'to such extent as is reasonable'. Furthermore, The Education Act 2011 gives wider search powers to tackle cyberbullying by providing a specific power to search for, and if necessary, delete inappropriate images or files on electronic devices.

Cogenhoe Primary School does not tolerate any form of bullying, inclusive of cyberbullying. Incidents of cyber bullying must be recorded and investigated as mentioned before, students should be aware not to delete or block anyone without collecting the evidence, taking down the URL or the username of the profile to help with further investigations. Any evidence found must be kept and filed and presented to outside agencies if necessary. The school will promise to take the correct steps to identify the bully: parents or guardians will be informed; monitoring undertaken to provide evidence where necessary and the Police contacted if there is a suspicion of a criminal offence.

School staff being targeted over the Internet

All school stakeholders have rights and responsibilities in relation to cyberbullying. Staff have the right to work free from harassment and bullying towards them that is carried out over the internet. Parents have the right to raise concerns about the education of their child, but should do so in an appropriate manner. The school has a right to encourage parents who are misusing social media to use it in an appropriate manner (DFE guidance 2014).

Staff are expected, under the Acceptable Use Policy, to ensure that their security and privacy settings on social media are set appropriately. Staff must also be aware that comments and images on social media sites may be visible to friends of social media friends, who may also be friends of parents and pupils. Annual discussion of the Acceptable Use Policy embeds these reminders to all staff.

Staff posting inappropriate comments on social media could lead to disciplinary action and having their employment terminated. Social media friends tagging staff in inappropriate posts, photographs or videos may also lead to disciplinary action, therefore staff are responsible for ensuring that their professional reputation is being upheld at all times. Staff must not give out personal mobiles or emails addresses to parents, even for school trips.

If a member of staff is subject to cyberbullying, this must be reported to a senior leader. Staff are encouraged to keep evidence. If the perpetrator is a current pupil, the school will follow the appropriate disciplinary procedures, as related in the Behaviour Policy. If a member of staff is involved in cyber bullying of another member of staff, then staff disciplinary procedures will be followed. If a parent is involved in cyberbullying of a member of staff, the Head will invite the parent into school to discuss their concerns. Advice will be given of the appropriate way to air their complaints, and a request will be made to remove the information, If the parent or carer refuses, the Head reserves the right to contact the West Northamptonshire County Council Online-Safety Officer, and if the comments are abusive, sexual or a hate-crime, the Police.

The Curriculum & Online-Safety

Using the internet is part of the curriculum and is a fantastic and necessary tool. Its use raises educational standards, and allows pupils to demonstrate responsibility and a mature approach. However, ~~I~~it is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Cogenhoe Primary School will have an annual programme of training which is suitable to the audience.

- Online-Safety for students is embedded into the curriculum; whenever computing is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.
- Key online safeguarding messages are reinforced whenever computing is used in learning.
- Our Computing scheme of work (Teach Computing and Barefoot Computing) incorporates lessons on online-safety. For KS1 children these lessons involve age-appropriate guidance, advice and discussion from the teacher; KS2 children, work through the online safeguarding units from the CEOP website (www.thinkuknow.co.uk) **or examples from 'Real Love Rocks.' (Upper Key Stage Two).**
- Pupils are made aware of copyright issues, data protection, intellectual property and reliability of information sourced on the internet as part of the curriculum.
- Pupils have opportunities for informal discussions about on-line risks and strategies for protecting yourself as part of the Online-Safety curriculum.
- Further to this, we have termly/yearly assembly exploring how to stay safe on the internet.
- Training or lessons are adapted as necessary in response to any incidents or inclusion of new media.
- All users understand that they must take responsibility for their network use.

Technology

Cogenhoe Primary School uses a range of devices including PC's, laptops, and tablets. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – SENSO and managed by NVP Team.

We use software that ensures that the school's infrastructure and network is as safe and secure as is reasonably possible. The Headteacher is ultimately responsible for ensuring all reasonable precautions are met in order to protect young users from inappropriate or harmful content. To date, the school has the following filtering measures in place:

- Filtering levels are managed in school via an administrations tool provided by our broadband supplier. Only the IT technician is authorised to allow access or block access to a site. These filters are age-appropriate.
- All users have unique usernames which ensures that they only have access to the appropriate level of filtering.
- Any changes to filtering levels are documented on the NVP logging system.

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. Thousands of inappropriate websites are created each day, and staff and pupils are trained on the protocols to follow if an inappropriate website is found, and pupils are supervised during internet sessions. Neither the school nor SENSO can accept liability for the material accessed, or any consequences of Internet access. An internet log is kept of inappropriate websites, and a report made to the appropriate agencies.

In addition to above, the following safeguards are also in place:

- **Anti-Virus** – All capable devices will have anti-virus software. This software is updated on a regular basis.
- **Email Filtering** – we use software that prevents any infected email to be sent from the school or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.
- **Supervision** – Pupils are supervised when using the internet and acceptable use policy is adhered to. An incident log will report breaches of filtering, and will be reported to the appropriate agencies
- **Passwords** – all staff and students will be unable to access any device without a unique username and password.
- **Staff –** should pre-view any websites for suitability before use, including those recommended to pupils for homework support as well as stimulus for other subjects.
- **Personal Data** – No personal data (as defined by the Data Protection Act 1998) is to leave the school; all devices that contain personal data are kept on school property and are password protected. Any breach is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
- **Password Protection –** staff should protect any documents that have full names, DOB, or data of children on in case of theft. These can be checked at any time.

Use of personal equipment

- Mobile phones must be kept hidden away and are only to be used when children are not in contact (staff room at lunchtimes or break times not in the classroom.)
- No devices such as smart watches that allow photos to be taken can be worn during school hours.
- No personal devices from home should be brought into school without the authority of HT and Computing Lead.

- If you bring in a device from home (not mobile) e.g. Ipad, tablet etc. once it has been authorised this must be declared to HT/Computing Lead so we are aware of your purpose.
- Your personal devices once declared and allowed must be connected to the school wifi to enable us to log inappropriate searches from your device.
- No photographs of the children should **ever** be taken on a personal device.
- All mobiles should be place in a secure place that can be locked and only is accessible by adults.

Safe use of school Computing equipment

- A log of Computing equipment is kept by the School Business Manager.
- Personal or sensitive data is not stored on school devices that can be removed from site.
- Serial numbers of all school equipment is logged and filed to protect against theft and for monitoring.
- Staff to request blocking of websites if we find any links we are unsure about and they can be investigated.

Mobile phones -

Pupil Use:

- The sending of abusive or inappropriate text messages is forbidden, and will be dealt with as part of our Cyber-bullying policy and coinciding with our Behaviour policy.
- All mobile devices/technology (including SMART WATCHES) should not be brought into school unless exceptional circumstances are made such as (MH) and this will still be handed to the office at the beginning of the day and collected at the end.
- Mobile phones and SMART WATCHES that are involved in any accusations of cyber-bullying can be accessed by the school with the parent's permission or the police is it is escalated.

Staff Use:

- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.
- Personal mobile technologies should not be used to contact children or families; nor should they be used to take videos or photos of pupils. School issued devices **only** should be used in these situations.
- Phones should not be present when children are around despite the reasoning for use; this is to protect ourselves and our pupils.

Visitors:

Visitors mobile phones and other technologies should be locked away in the lockers provided and should not be taken out and used anywhere except the staff room. No personal devices will be allowed to be used unless there is previous authorisation.

Parents:

Parents should not have the use of personal devices while inside the school building. Parent visitors should lock away their phones and other mobile devices in the lockers provided. Parents will only be allowed devices on performances or celebration assemblies to allow them to film their child. The Head teacher will express that photos and videos may be taken but not to be posted onto any social media.

Internet

- Use of the internet in school is a privilege, not a right. All staff must sign the staff Acceptable Use Policy.
- Pupils and parents will all receive a copy of the Student Acceptable Use Policy as well as the key stage rules, and understand that unacceptable use may mean withdrawal of internet privileges.

Email

- The school gives all staff their own e-mail account to use for school business to protect staff. All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted.

- It is not permitted nor advised to send emails to parents from a personal account.
- Students have their own email but it is not being used as a form of communication, but they do have access to TEAMS chat via this. NVP can disable and monitor the chat.

Published content and the school web site –

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate however each year group will also be held responsible for their year groups page.
- The security of staff and pupils is paramount. The Head Teacher takes responsibility for ensuring that pupils are protected and full names of pupils are not published alongside photos. Parents give written consent for images of their children to be used on the school website.
- Those children who are not permitted are logged and filed, and staff are aware of these children in their classrooms.
- School leaders promote the privacy of pupils on school events such as sports days and class assemblies.

Photos and videos

- Digital media, such as photos and videos, are covered in the schools' Photographic Policy. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.
- Class assemblies and Christmas performances are always introduced by the Headteacher or Deputy Head. This introduction is inclusive of reiterating to parents that photos and videos are for their own personal use and must not be published on social media.

Social Networking

- The school has a Facebook page, however, security settings are set so nobody can comment or message the account regardless of if they have liked the page or not.
- No photos will be published to the school Facebook page and will only be accessible via website links.
- To maintain the school's reputation staff are expected to maintain professional conduct on all social media sites. They are requested not to become friends with parents, unless there are particular circumstances, such as their children attend the school. Even in these situations, staff are requested that they must not comment on posts, which may reveal the identity of other staff to other parents.

Incidents

- Any online-safety incident is to be brought to the immediate attention of the DSL Team, Computing Lead, or in his/her absence the Headteacher. The Computing Lead and DSL Team will assist stakeholders in taking the appropriate action to deal with the incident and to fill out an incident log on EDUKEY

Parents

- The Online-Safety policy and any other parental online-safety information are available on the school website
- Parents are encouraged to read the school Acceptable Use Policy, the Key Stage rules and there are presentations available for the parents to view if they are unsure of the concept of Online-Safety.
- Parents will receive a copy of digital parenting magazine, receive regular emails concerning online safety and how to help at home, Workshops will also provide parents with recommendations of apps to help them understand what their children are doing online and how to prevent issues arising.

Emerging technologies

Online-Safety is an ever evolving area and is always developing as things are constantly developing. The school will take all reasonable precautions to identify and minimise risk from emerging technologies.

- Emerging technologies will be examined for risk and an educational assessment carried out before school use. As well as this, restrictions or filters are embedded before the technology is implemented for pupil use.
- Pupils are regularly instructed and reminded on the safe and appropriate use of technology and personal devices on and off site in accordance with acceptable use policies.

Acceptable Use Policy – Staff

You must read this policy in conjunction with the Online-Safety Policy. Once you have read and understood both, you must sign that you have read and agreed to the Acceptable Use Policy. This policy forms part of the terms and conditions set out in your contract of employment.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online-safety incident, reported to the Computing Lead and DSL Team and an incident log on EDUKEY completed. Any incidents may result in disciplinary action and may need to be reported to the Police

Social networking – Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not seek to become "friends" with parents or pupils on personal social networks. It is understood that there may be existing relationships of staff living in and around the village, but these must be open & disclosed to the Head teacher and the Child Protection Officer.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act. You must not email a parent for a professional matter via your personal account.

Passwords - Staff should keep passwords private.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that no data concerning personal information is taken offsite. If it is necessary to take sensitive data off-site, permission should be gained from the Head teacher and the information must be encrypted (e.g. on a password protected memory stick).

Personal Use of School devices - You are not permitted to use equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of other staff without consent. This is applicable professionally (in school) or personally (i.e. staff outings). The school must be supported in its approach to online safety and staff must not deliberately upload any images or videos that could upset a member of the school community. Images and videos of children who have permission should not be published anywhere but the school website which will be managed by the headteacher.

Professional Role –Staff should ensure that all online activity, inside and outside school, will not bring themselves, colleagues or the school into disrepute.

Use of Personal devices - use of personal equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the Computing Lead. Phones should be locked away and only accessed in the staff room.

Viruses and other malware - any virus outbreaks are to be reported to IT support as soon as it is practical to do so, along with the name of the virus (if known).

Online-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive online-safety messages in all use of computing whether you are with other members of staff or with students.

Note – All users are reminded that Internet activity may be monitored without prior notice. This is in order to ensure, as much as possible, that users are not exposed to illegal or inappropriate websites, and to ensure, as much as possible, that users do not actively seek access to illegal or inappropriate websites.

Cogenhoe
Primary School

Our Online Rules

Key Stage 2

Cogenhoe pupils will:

- Be aware of all the different uses of the internet and how to stay safe in all software, programmes and tools.

- Do **NOT** speak to strangers online or usernames you do not recognise, they may not be who they say they are.

- Only send messages that are kind and polite.

- Not go on any website or internet tools such as video conferencing without our parents being aware of when we are on it and who we are talking to.

- Not give out personal information such as name, school, address or phone number. Alongside this, the children will also provide 'gamer tags' on games as opposed to any direct link to their information.

- Will not post any photos of yourself or others on any 'apps' that you would not want a stranger to see.

- Will not post photos of others, if they want to post it then can do it themselves, permission or no permission.

- Know who to ask/talk to if they received any content that makes them feel uncomfortable.

- Know how to report/block content we are uncomfortable with, or which we no longer wish to receive, but to screenshot evidence before deleting messages.

- Follow these rules as part of an agreement and be aware of the dangers and consequences that could be implicated if they do not.

Our Online Rules

Key Stage 1

Cogenhoe pupils will:

- Use the internet safely to protect ourselves, and keep us safe.
- Not go on any website or internet tools such as video conferencing without parents/carers being aware of when we are on it and who we are talking to.
- Only open or send messages with the supervision of an adult to people we know, none of which should be unkind messages. Do not speak to people you do not know, even if you have spoken for a long time.
- Not tell anyone their first name, last name, school or address. This is YOUR information, and it must not be told to anyone else.
- Not tell anyone their password, your user area is yours and no one else should access it.
- Talk to an adult if they see something they do not like, or something that makes us feel uncomfortable.
- Block or report someone who is being unkind, or doing things you do not want to see but ask an adult to collect evidence first.
- Follow the online rules, and are aware of the dangers it can have and the consequences they will face

Computing Risk Assessment Log

DISCLAIMER: The school will take all reasonable precaution to ensure that users access only appropriate material. However, due to the internet and social media being so vast, it is not possible to guarantee that access to undesirable material will never occur. The school cannot accept liability for the material accessed, or any consequence resulting from the internet use.

No.	Activity	Risk	Likelihood	Impact	Owner
1.	Internet browsing	Access to inappropriate/illegal content – staff	1	3	e-Safety Officer IT Support
2.	Internet browsing	Access to inappropriate/illegal content – students	2	3	

Likelihood: How likely is it that the risk could happen (foreseeability).

Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.

Owner: The person who will action the risk assessment and recommend the mitigation to the Headteacher and Governing Body.

The final decision rests with Headteacher and Governing Body

End of document