St Giles C.E. Primary School
Online Safety Policy

Introduction

The Online safety Policy relates to other policies including those for Computing, bullying and for Safeguarding.
The designated safeguarding leaders for the school are Mr Mark Dakin and Mr Les Dow.

The school's named Online Safety Leads are:

Online Safety Lead - Mr D Hatfield

Online Safety Governor – Mrs N Hylton

Our Online safety Policy has been written by the school, building on advice received and government guidance. It works in conjunction with the school devised acceptable use policy. It has been agreed by senior management and approved by governors.

Created: September 2025
The next review date is: September 2026

The school will monitor and enforce the policy through:

- Lightspeed - advanced monitoring that is moderated by vast AI technology and human specialists. Schools are alerted immediately should an incident arise.
- Teacher planning and delivering of the curriculum (through the use of Project Evolve)
- Log of any incidents: Mr M Dakin, Mrs S Mavi, Mr L Dow and Mrs L Leonowicz monitor behaviours
- Technical Staff from Services for Schools to ensure all security software, including virus software and settings are kept up to date

Every member of the school community has a duty of care to online safety as part of safeguarding. This policy deals with incidents associated with the use of technology that affects our school community.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the Online safety Policy. In accordance with KCSiE September 2025 Governors should ensure they have had training on an annual basis about online safety.

School responsibility

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Keeping Children safe in Education September 2025 states 'All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content.'

Incidents

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

• content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, misinformation, 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: personal 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; and

• commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams

Monitoring Software

Lightspeed is used across the network in order to

- Monitor inappropriate use of language
- Monitor internet usage, including words associated with the prevent agenda
- Enforce the agreement of the Acceptable Use Policy (See Appendix 1)

Any identified incident is reported to Mr M Dakin and Mr L Dow in order for it to be investigated and dealt with.

Managing filtering

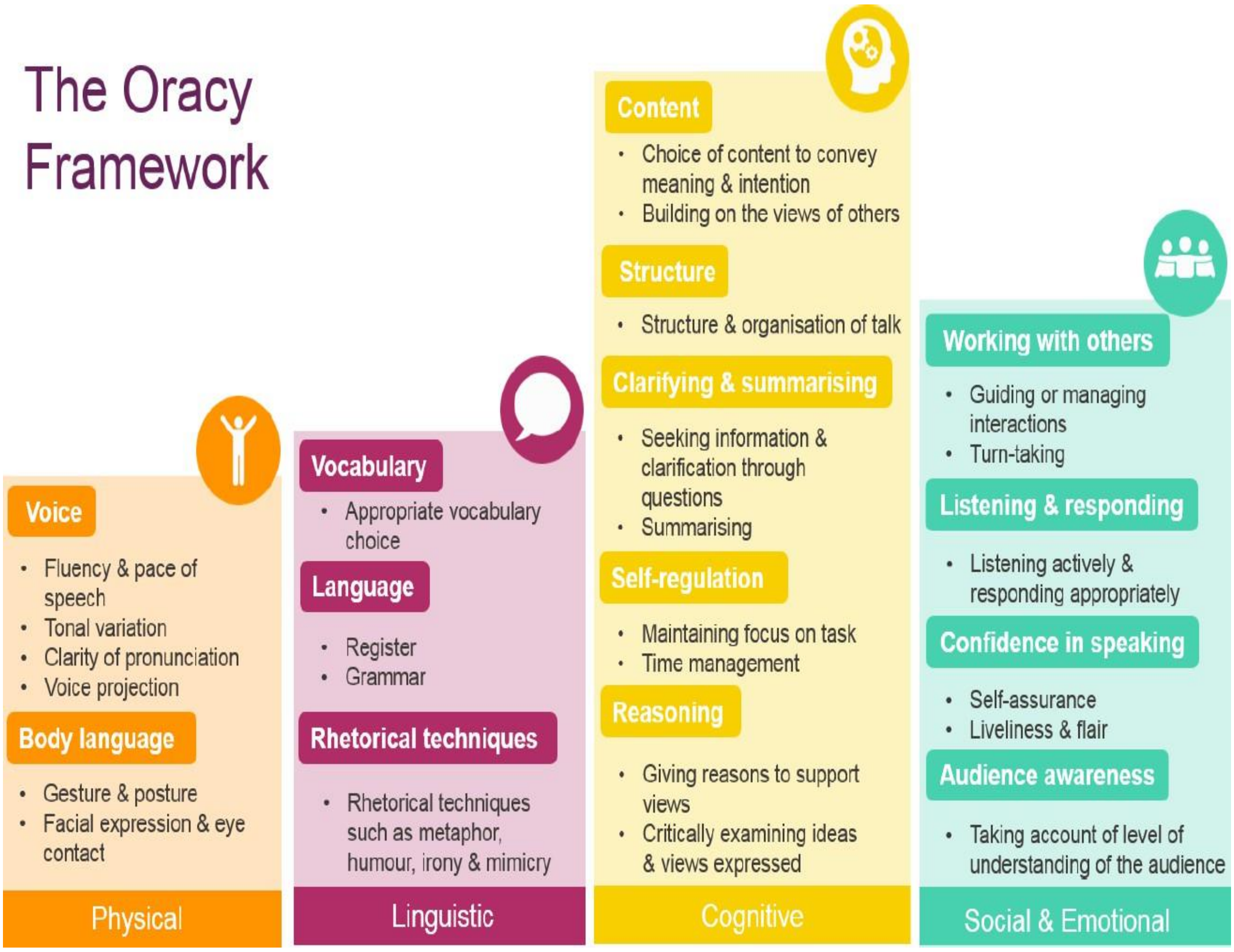
If staff come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator. If pupils come across unsuitable on-line materials, the site must be reported to their teacher who will inform the Online Safety Coordinator. Staff are now able to access sites such as 'You Tube' and others on request but staff need to be aware that these sites do contain inappropriate materials and therefore children are not allowed to use these sites. **Links and content should be shared and checked in school by staff just prior to use in the classroom due to daily rotation of advertising content.**

Reporting incidents

The school use My Concern to record incidents of online safety in line with the Child Protection policy.

Online Safety in the curriculum

A programme of training in Online Safety will be taught to children across the school from Nursery to Year 6. The school uses a combination of activities from Education for a connected world and Project Evolve. (See Computing and Online Safety Curriculum Overview). This is taught through the Computing and PHSE curriculum. This is also underpinned by our Oracy policy.



The Oracy Framework

Physical

Voice
- Fluency & pace of speech
- Tonal variation
- Clarity of pronunciation
- Voice projection

Body language
- Gesture & posture
- Facial expression & eye contact

Linguistic

Vocabulary
- Appropriate vocabulary choice

Language
- Register
- Grammar

Rhetorical techniques
- Rhetorical techniques such as metaphor, humour, irony & mimicry

Cognitive

Content
- Choice of content to convey meaning & intention
- Building on the views of others

Structure
- Structure & organisation of talk

Clarifying & summarising
- Seeking information & clarification through questions
- Summarising

Self-regulation
- Maintaining focus on task
- Time management

Reasoning
- Giving reasons to support views
- Critically examining ideas & views expressed

Social & Emotional

Working with others
- Guiding or managing interactions
- Turn-taking

Listening & responding
- Listening actively & responding appropriately

Confidence in speaking
- Self-assurance
- Liveliness & flair

Audience awareness
- Taking account of level of understanding of the audience

Early Years Foundation Stage and Key Stage 1

At this level, use of the Internet will either be quite heavily supervised or based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Lower Key Stage 2

Children will now be given more opportunities to develop their digital literacy skills (e.g. sending polite and friendly messages online to other children, the need to create strong passwords etc). They will be shown how to develop a responsible attitude towards searching the World Wide Web and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Upper Key Stage 2

Children will now be encouraged to become more independent, agreeing to the acceptable use policy first, before searching for information on the World Wide Web using a child friendly search engine, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult. Children will also be taught about appropriate use of AI, with regards to plagiarism and creating harmful, hurtful or distasteful content.

Parents and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. St Giles Primary will take every opportunity to help parents understand these issues through parents' evenings, 'meet and greets', weekly newsletters, letters, web site and information about national / local Online Safety campaigns. Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / pupil records
- their children's personal devices in the school (where this is allowed)

Where an incident occurs within school the child's parents will be given appropriate advice for the use of technology at home.

Visitors to school

Whilst the nature of a visitor's Internet use will clearly vary depending upon the purpose of their visit, it is still important to explain the school's expectations and rules regarding safe and appropriate Internet use to them. These differ slightly to those given to pupils to acknowledge the different situations in which visitors will likely be using the Internet:

- I will respect the facilities on offer by using them safely and appropriately.
- I will not use the Internet for: personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect myself and others.
- I will not download/install program files to prevent data from being corrupted and to minimise the risk of viruses.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details for websites with others.
- I will not carry out personal or unnecessary printing when using the Internet due to the high cost of ink.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

E-communication within school

Pupils may only use approved electronic communication accounts on the school system. (E.g. email). Children will be told they must immediately save and tell a teacher if they receive an offensive message.

Staff should use a school email communication for anything work related and no other email address. The forwarding of chain communications is not permitted.

Personal use

Staff all have access to networked computers and Chromebooks. These are given for professional use only and should not be used for inappropriate activities. (Please see section below)

Mobile devices

The use of mobile devices including mobile phones and smartwatches should not be used in classrooms and teaching areas especially during the school day (8.30 - 3.30) excluding lunchtimes in the staff room, and only used on school trips away from children in an emergency. All devices should be silenced during school hours.

Pupil devices should not be used during the school day. Year 6 pupils are allowed to bring in mobile phones if they are walking to or from school alone, these must be collected or handed into the class teacher so they cannot be used during school time.

Remote education

Remote education is included in our safeguarding considerations - please consult our remote learning policy for more information.

Data protection

Please refer to the schools Data Protection policy for further information.

Staff should be using password protected storage systems for transfer of files e.g. password protection on Google drive / Microsoft One Drive.

Social networking and personal publishing

The school will control access to social networking sites, they will be restricted as appropriate. Pupils will be educated in the safe use of such sites alongside the use of relevant child friendly websites.

Pupils, staff and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Pupils will be advised to use nicknames and avatars when using social networking sites. Staff must not make 'friends' or communicate with current pupils or pupils that have left on any social network site, i.e. Facebook, Instagram. Staff should check that their privacy setting is set to 'Friends only' and consider changing their profile name. Staff who choose to use 'Facebook' and other network sites do so at their own risk and should be aware of the School's Code of Conduct.

Pupils will be taught when 'gaming' i.e. on PlayStation, Xbox, Nintendo or PC, they should only communicate with people they know rather than unknown gamers and play age appropriate games.

Managing 21st century technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. **School staff should be aware that mobile technologies with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.**

Personal devices, including mobile phones, will not be used during lessons or formal school time unless express permission is given by the Head or Deputy Head. Personal devices must not be accessed (e.g. in another room or locked away) when children are present. The sending of abusive or inappropriate messages or files by Bluetooth or any other means is forbidden. Staff will be issued with a school phone where contact with pupils or a parent is required. **Staff will not use personal devices to capture images/videos of pupils.**

Protecting personal data and cybersecurity

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Refer to the School's data handling policy. Staff should use Google Drive / One Drive or the school server. Ideally this should be the only form of data storage that staff use. If they do use memory sticks they must encrypt them in order to store any personal data relating to work that needs to leave the school premises. **Staff should ensure that the device is not left unattended. Staff should not walk away from any device without first locking it.**

Password security

Staff are responsible for managing their own passwords for the network and websites used as part of school life but should be mindful of what they are using as passwords. Three random words with a mixture, numbers and punctuation is the recommended password format. All passwords should be different for every site or programme. Staff are encouraged to use password managers.

Pupil passwords should be kept in pupil reading diaries. For EYFS these should be easy to type and unique for each pupil. KS1 and KS2 pupils use year of entry - surname - initial and a generated password for them.

Network passwords and associated apps or sites are managed by the school technical support team.

School network security

The school is supported by Services for Schools technical support who maintain and support the school with antivirus and technical network security. All incidents of this nature should be reported to them in the first instance.

Authorising Internet access

Parents will be asked to sign and return a consent form on a yearly basis.

Handling Online safety complaints

Complaints of internet misuse will be dealt with by an e safety coordinator or the Head. They need to be recorded on an e-safety incident form. (See appendix three) Any complaint about staff misuse must be referred to the head teacher or LADO (contacted via Walsall MASH on 0300 555 2866)
Complaints of a safeguarding nature must be dealt with in accordance with school's safeguarding procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet.

Staff and the Online Safety policy

All staff will receive in house Online Safety update training on an annual basis. Staff are informed that network and internet traffic will be monitored and can be traced to the individual user. Staff will always use a child friendly safe search engine when accessing the web with pupils, for example www.swiggle.org.uk

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupil Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X			X	X		X
Unauthorised use of non-educational sites during lessons	X				X		X	
Unauthorised use of mobile phone / digital camera / other handheld device	X	X			X		X	
Unauthorised use of social networking / instant messaging / personal email	X	X			X		X	
Unauthorised downloading or uploading of files		X		X	X		X	
Allowing others to access school network by sharing username and passwords	X	X			X	X		
Attempting to access or accessing the school network, using another student's / pupil's account	X	X			X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X			X	X		
Corrupting or destroying the data of other users		X			X	X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X			X	X		X

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X	X		X
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X			
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X		X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X		X	X	X	X	

Staff Incidents/Sanctions:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X		X	X	X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		X			X	X		
Unauthorised downloading or uploading of files		X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X							

Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		X			X	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X		X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X	X			X	X	X
Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		
Using proxy sites or other means to subvert the school's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Continued infringements of the above, following previous warnings orsanctions								X

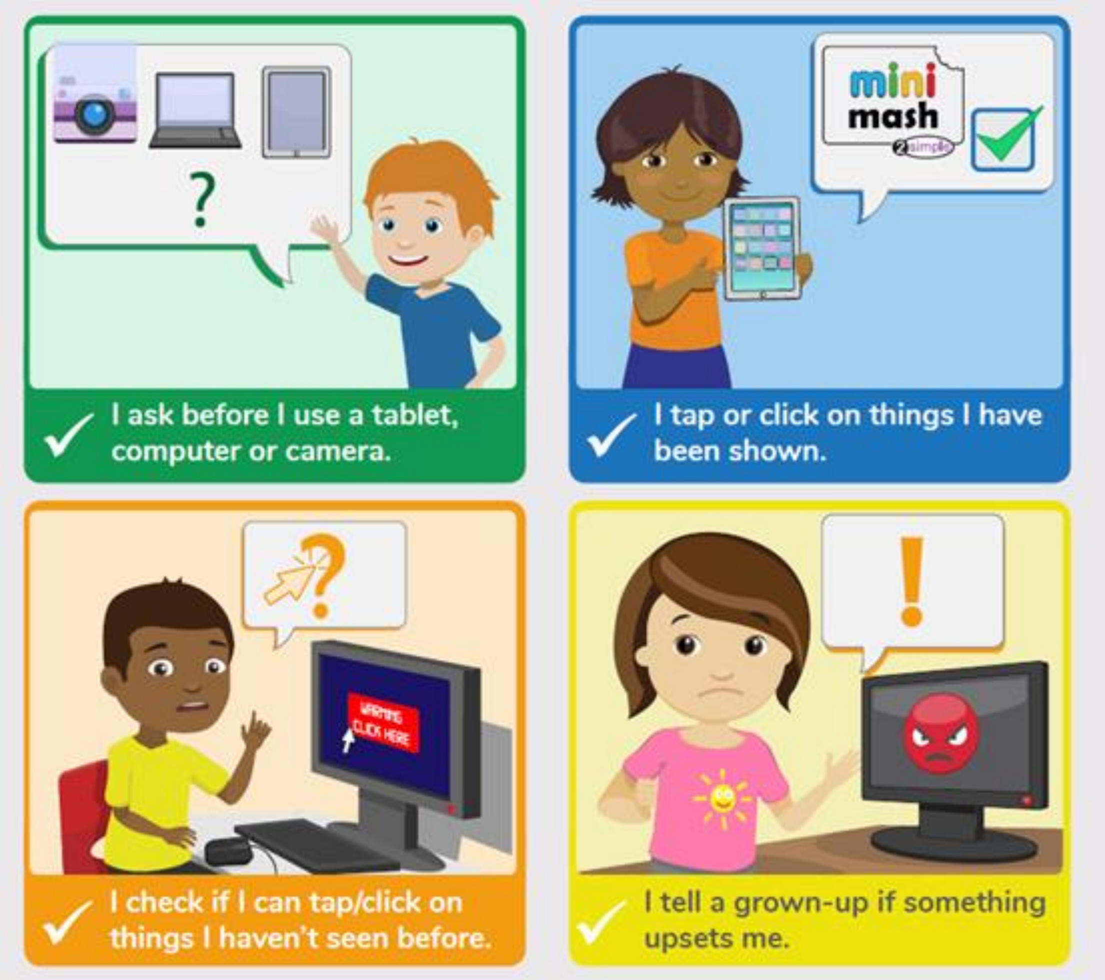
Reviewing online safety practice in school

The school proudly holds the SWGFL 360 safe Online Safety mark. The Online Safety Lead is responsible for keeping up to date on all online safety issues and ensuring that staff are updated as necessary, they also regularly review the online safety provision with RoarTech.

To be reviewed September 2026

Appendix One

ICT Agreed Usage Plan EYFS


?
✓ I ask before I use a tablet, computer or camera.
mini mash
2simple
✓ I tap or click on things I have been shown.
WARNING CLICK HERE
✓ I check if I can tap/click on things I haven't seen before.
!
✓ I tell a grown-up if something upsets me.

ICT Agreed Usage Plan KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

I am aware of the CEOP report button and know when to use it.

Signed: __________________________ (pupil) Signed: _______________________(parent)

CEOP REPORT
ceop.police.uk

ICT Agreed Usage Plan KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

○ always keep my passwords safe

○ only use, move and share my personal data securely

○ only visit sites which are appropriate

○ work in collaboration only with people my school has approved and will deny access to others

○ respect the school network security

○ make sure all messages I send are respectful

○ show a responsible adult any content that makes me feel unsafe or uncomfortable

○ not reply to any nasty message or anything which makes me feel uncomfortable

○ not use my own mobile device in school unless I am given permission

○ only give my mobile phone number to friends I know in real life and trust

○ only email people I know or approved by my school

○ only use email which has been provided by school

○ obtain permission from a teacher before I order online

○ discuss and agree my use of a social networking site with a responsible adult before joining

○ always follow the terms and conditions when using a site

○ always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)

○ always check with a responsible adult before I share images of myself or others

○ only create and share content that is legal

○ never meet an online friend without taking a responsible adult that I know with me

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Signed: ___________________________ (pupil) Signed: ______________________(parent)

School Staff ICT Agreed Usage Plan

I agree that I will:

- ○ only use, move and share any personal data securely using password protected devices
- ○ respect the school network security
- ○ implement the schools policy including the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- ○ respect the copyright and intellectual property rights of others
- ○ Use work devices for work purposes
- ○ only use approved email accounts
- ○ only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- ○ only give permission to pupils to communicate online with trusted users.
- ○ use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- ○ not use or share my personal (home) accounts/data (e.g. Facebook, email, eBay etc) with pupils/parents who I have no family or strong outside school friendship with: (if you wish to make these connections with anyone you must have specific permission of the Headteacher)
- ○ Ensure full privacy options are used on social networking sites
- ○ set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters (upper & lower case), numbers and other permitted signs).
- ○ report unsuitable content and/or ICT misuse to the named online safety officer
- ○ promote any supplied online safety guidance appropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will not:

- ○ visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

○ pornography (including child pornography)
○ promoting discrimination of any kind
○ promoting violence or bullying
○ promoting racial or religious hatred
○ promoting illegal acts
○ breach any Local Authority/School policies, e.g. gambling
○ do anything which exposes others to danger
○ any other information which may be offensive to others
○ forward chain letters
○ breach copyright law
○ use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
○ store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed:___________________________________

Job Title: ___________________________________

Date:___________________________________