September 2024

Stokes Wood
Primary School

Online Safety Policy

Development / Monitoring / Review of this Policy

This policy has been written in consultation with staff, governors and parents at Stokes Wood Primary School.

Key staff referred to throughout the policy are DSLs (Head teacher, Assistant Headteacher, Learning Behaviour Mentor) and Computing/Online Safety lead.

Online safety governor is the safeguarding governor.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys/questionnaires of stakeholders

It will be reviewed annually as part of the school's safeguarding review.

Schedule for Development / Monitoring / Review

This online policy was approved by the Governing Body on:	February 2019 Reviewed September 2019 Reviewed April 2020 Reviewed September 2021 Reviewed September 2022 Reviewed September 2023 Reviewed September 2024
The implementation of this online policy will be monitored by the:	SLT
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the online policy generated by the monitoring group (which will include anonymous details of online incidents) at regular intervals:	Annually
The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online or incidents that have taken place. The next anticipated review date will be:	September 2025
Should serious online incidents take place, the following external persons / agencies should be informed:	Leicester City Social Services. Leicester Safeguarding Board, Police as appropriate

Contents

1. Statement of Intent

The online safety policy is intended to demonstrate the organisation's commitment to:

- Ensuring the safety and wellbeing of children, young people and adults is paramount when using the internet, social media, or mobile devices.
- Providing staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensuring that, as a school, we operate in line with our values and within the law in terms of how we use online devices.

This policy applies to all members of Stokes Wood Primary School including staff, pupils, governors, volunteers, parents, carers, visitors, and community users who have access to and are users of digital technology systems, both in and out of the school.

2. Linked Policies

This online safety policy should be read alongside our organisational policies and procedures, including:

- Acceptable Use policy (KS1 & KS2)
- Anti-Bullying Policy (including Cyberbullying)
- Child on Child, Sexual Violence and Harassment Policy
- GDPR Data Protection Strategy
- RSE and Health Education Policy
- Safeguarding and Child Protection Policy
- Behaviour Policy
- Social Media Policy
- Special Educational Needs and Disability Policy

Staff related Policies and Procedures:

- Acceptable Use policy
- Disciplinary Policy and Procedure
- Social Media Policy
- Staff handbook which includes Staff Code of Conduct

The above list is not exhaustive but when undertaking development or planning of any kind the school will consider the implications for online safety.

3. Roles and Responsibilities

The school takes a whole-school approach to online safety and all stakeholders are responsible for ensuring that effective policies and procedures are maintained and upheld. It is expected that all staff and volunteers read and understand this policy and implement it consistently.

3.1 Governors:

Governors play an important part in monitoring the online safety provision across the school. They are responsible for:

- Reviewing and approving this policy.
- Reviewing data and reports from Online Safety and Pastoral Lead

- Appointing a designated governor with oversight of safeguarding and online safety. It is the role of the lead governor to meet with the Online Safety and Pastoral Lead regularly to ensure any weaknesses are addressed.
- Agreeing and adhering to the terms on acceptable use of the Trust's ICT systems and the internet.
- Developing individual knowledge and understanding to ask the right questions and professionally challenge and test what happens across the school.

3.2 Headteacher and Senior Leaders:

The headteacher and senior leaders take overall responsibility in ensuring that all staff and pupils understand and follow the policies and procedures of online safety. Key responsibilities:

- Ensuring all staff understand this policy and that it's implemented consistently.
- Reviewing the school's infrastructure/network with Technical Support to ensure it is safe and fit for purpose.
- Delivering online safety training to all members of members of the school community.
- Ensuring that there are robust protocols in place for both monitoring and reporting online safety issues.
- Ensuring all staff adhere to the policies and procedures around online safety. E.g. acceptable use policy.
- Knowing the procedures in the event of serious online safety allegations against a member of staff.

3.3 Online Safety and Pastoral Lead:

This role is part of the school's Designated Safeguarding Lead team. The Online Safety DSL will be trained on online safety issues and be aware of the potential for serious child protection/ safeguarding issues. Key responsibilities:

- Having a responsibility for online safety issues in school.
- Liaising with external agencies where necessary.
- Providing regular reports on online safety in school to the headteacher and governors.
- Keeping up to date with current legislation, developments, and resources.
- Providing training and advice for all staff across school.
- Taking a lead role in personalising policies/documents.
- Attending any relevant meetings with governors and updates them on progress of online safety.
- Ensuring pupil voice is considered as part of online safety development/strategy.
- Ensuring all online safety incidents are logged onto CPOMs, providing training for staff where necessary.

The online safety leads at Stokes Wood Primary School are James Smith and Megan Williams.

3.4 Network Manager/ Technical staff:

The technical support staff play a huge role in ensuring pupils are kept safe. They are responsible for:

- Ensuring that school networks are secure and safe to use.
- Monitoring the school networks and internet regularly.
- Implementing and updating monitoring software/systems are as requested by Online Safety and Pastoral Lead.
- Ensuring that only authorised users can access the network and these users adhere to the schools guidance on password protection.

- Ensuring that they keep up to date with relevant online safety updates.
- Ensuring that filtering policies are applied to the correct users.
- Ensuring that any filtering request changes are liaised and agreed with Online Safety and Pastoral Lead before actioning.
- The management of Office365 and ensuring policies and procedures are being followed.

3.5 Teaching and Support Staff:

Teachers and support staff are the day-to-day contact for pupils and therefore responsible for promoting safe online safety behaviour. Key responsibilities are:

- Ensuring they attend any relevant training that is issued by the headteacher or Online Safety Lead.
- Ensuring that they adhere to the policies and procedures relating to online safety. E.g., acceptable use policy, staff handbook.
- Supporting pupils with their understanding and ensuring they follow online safety procedures and policies.
- Ensuring that where there is pre-planned internet use, pupils are guided to sites that are suitable.
- Reporting any online safety concerns to the online safety lead.
- Ensuring policies around mobile phones are enforced with all pupils.
- Ensuring digital communications with pupils/parents/carers on carried out using official school systems and that conversations always remain professional.
- Ensuring a online safety curriculum is delivered to all pupils.
- Ensuring all online safety issues are embedded into all aspects of the curriculum.

3.6 Pupils

Pupils are responsible for:

- Ensuring that they use the digital technology systems in accordance with the pupil acceptable use policy.
- Understanding the importance of reporting abuse, misuse or access to inappropriate material.
- Adhering to mobile phone guidance and are aware of the consequences if they don't follow this.
- Understanding the need for good online safety behaviour both in and out of school.
- Providing valuable feedback about online safety through surveys and discussions.

3.7 Parents/Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media, and information about national/local online safety campaigns/literature. 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.
- Online learning platforms (Century, Purple Mash, Google Classroom)
- Their children's personal devices (where this is allowed).

3.8 Community Users

Community users who have access to the school systems or programmes as part of the wider school provision will be expected to sign a Community User Acceptable Use Policy/Agreement before being provided with access to school systems. This will be done as they enter the building using our sign-in system**.**

4. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet. The Online Safety Lead has overall responsibility for the school's approach to online safety, with support from the school's senior leadership team, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The importance of online safety is integrated across all school operations in the following ways:

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

5. Online Safety in the Curriculum

We want our pupils to take responsibility and act in a responsible way. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across all subjects where relevant. The online safety curriculum used is SWGfL Project Evolve and is broad, relevant and provides progression, with opportunities for creative activities.

Online safety awareness will be provided in the following ways:

- A planned online safety curriculum (SWGfL Project Evolve) which is delivered through computing and PSHE lessons, as well as being reinforced through all parts of daily school life.
- Key online safety messages are reinforced as part of a planned programme of assemblies and themed Online Safety focused weeks, including Internet Safety Day and Wellbeing Week.
- Pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Schools are required to ensure all devices have monitoring software on them that detects and alerts the school of any potential exposure to extremism.

- Pupil's will be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will act as good role models in their use of digital technologies, the internet, and mobile devices.
- In lessons where internet use is pre-planned, staff will ensure that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

6. Parent awareness and working with the wider community

We understand that many parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of children's online behaviour. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will provide information and awareness to parents and carers through:

- Curriculum activities, themed online safety awareness weeks. High profile events/ campaigns e.g Safer Internet Day and Wellbeing Week.
- Letters, school newsletters, school website
- Open evenings/Parent workshops
- Online Safety assemblies

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.
- Sharing their online safety expertise/good practice with other local schools.

All parents sign an acceptable use policy on behalf of their children when they join the school and then re-sign annually. (Appendix 1)

7. Training

It is essential that all staff (including governors)receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training is made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.

8. Online Safety Concerns

8.1 Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating, or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging apps (e.g. WhatsApp)

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

8.2 Child on child abuse

Pupils may use the internet and technology as a vehicle for sexual abuse and harassment towards each other. The following are examples of online harmful sexual behaviour:

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

The school will respond to all concerns regarding online child on child abuse and DSLs will investigate the matter in line with their Child Protection and Safeguarding Policy.

8.3 Grooming

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them. Staff are aware that grooming often takes place online where the perpetrator will often hide their identity through pretending to be someone they are. Pupils are less likely to report grooming behaviour because:

- The pupil believes they are talking to another child
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

The school will respond to all concerns regarding grooming and DSLs will investigate the matter in line with their Child Protection and Safeguarding Policy.

8.4 Child Sexual Exploitation (CSE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider

network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

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

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

8.5 Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda.

Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Where staff have any concerns about pupils being radicalised, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Prevent Duty and Child Protection and Safeguarding Policy.

8.6 Cyber-Crime

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

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

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime.

Where there are any concerns about a pupil's use of technology and their intentions about using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

8.7 Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage please refer to Appendix 2.

9. Responding to Online Incidents

9.1 Responding to Pupil Incidents:

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident. The schools DSLs will determine the seriousness of all incidents and report all illegal activities/incidents to the appropriate organisation, these include:

- Police
- CEOP (child exploitation and online protection)
- CyberChoices

Appendix 3 gives examples of different scenarios and who these should be reported to in the first incidence.

9.2 Responding to staff incidents

Where a staff member misuses the school's IT systems or internet or uses a personal device in a way that their actions constitute in misconduct, then the matter will be dealt with in accordance with the staff disciplinary procedure. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police. A flow chart in dealing with illegal activity (Appendix 4) supports the school in taking the correct action.

10. Filtering and Monitoring

Stokes Wood Primary School recognises that filtering and monitoring plays a huge role in safeguarding it's pupils and has accessed it's systems against the DFE's Meeting digital and technology standards in schools and colleges.

The school has reviewed these standards to ensure the specifications have been met. This includes:

- Ensuring a member of senior leadership and governor is responsible for ensuring standards are met.
- The Online Safety Leads work alongside technical support staff to ensure filtering and monitoring meets the standard.
- The school uses iboss filtering system and this is regularly checked to ensure it is blocking illegal content including child abuse material (CSAM).
- The school uses Securus as a monitoring system and regularly to ensure that it is effective in safeguarding its pupils.

11. Smart and Mobile Technology

The school understands that the rapid development of smart and mobile technology possesses an ongoing online safety risk to pupils. The development of mobile devices and smart watches has meant that pupils are 'online' 24 hours a day.

11.1 Pupils

For pupils in Year 5 and 6, if they walk home alone, they can bring in a mobile phone however this must be put into the designated class lock box as soon as they arrive at school. Mobile phones will then be given back to pupils at the end of the day by a member of staff.

Pupils are not permitted to wear smart watches in school. Pupils who come to school wearing smart watches will be asked to remove these. They will be kept in the office and returned to parents/carers at the end of the day.

11.2 Staff and Governors

Staff members must not use a personal device (e.g., phones and tablets) throughout the school day, unless this is in their own break/lunch time. Staff are not permitted to take or store images of pupils on their mobile device. Personal information about staff, pupils, or the school is not to be stored on any personal device.

Personal mobile phones must not be used to contact pupils or parents. During school outings, nominated staff will have access to a school mobile phone which can be used for emergency or contact purposes.

Staff can wear smart watches however it must be put on airplane mode. If staff are using smart features they will be asked not to wear the watch again in school. Please see the staff code of conduct.

12. Remote learning

All remote learning is delivered in line with the school's Home Learning Protocol Policy. The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, Securus monitoring software installed, has working audio and video and can download documents where appropriate.

The school is not responsible for ensuring that devices that go home have strict filtering installed and this is the responsibility of the parent/carer to ensure safe use. During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software and filtering, on devices not owned by the school.

13. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Care will be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' work can only be published with the permission of the pupil and parents or carers.

14. Communications

When using communication technologies the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored.
- Staff must only use the school email service or Microsoft Teams to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the Headteacher – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

15. Social Media

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their

employees in the course of their employment. Staff members must adhere to the staff social media policy.

15.1 School's social media platforms:

The Office Manager controls the school Facebook and X (formally twitter) accounts. No one else is able to post on behalf of the school at present. The office manager consults with the head teacher and Online Safety Leads on the content of posts from school and from parents.

16. Policy review

This policy will be reviewed by school Online Safety Leads annually and updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

Appendix 1 – Acceptable Use Policy

Stokes Wood Primary School

ACCEPTABLE INTERNET USE STATEMENT FOR PUPILS AND STAFF

Parents/Carers of pupils should sign a copy of this Acceptable Internet Use Statement and return it to the school where it will be countersigned by a member of staff. Failure to read and complete this form will restrict the use of the computers in school for your child. *Thank you for your co-operation.*

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school has an Internet Access Policy (see below) and Online Policy (on school website) drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- Access should only be made via the authorised account and password that should not be made available to any other person.
- The security of the ICT system must not be compromised whether owned by the school, by Leicester City Council or any other organisation or individual.
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Users are responsible for all email and messages sent and for contacts made that may result in email being received.
- The same professional levels of language and content should be applied as for letters or other media, particularly as email is often forwarded.
- Posting anonymous messages and forwarding chain letters is forbidden.
- **Cyber bullying, using abusive and unkind comments is forbidden.**
- Copyright of materials and intellectual property rights must be respected.
- All Internet use should be appropriate to staff professional activity or to student's education. However please note that:-
  - The school's ICT system may be used for private purposes following guidelines established by the school.
  - Use for personal financial gain, gambling, political purposes or advertising is forbidden.
  - The use of social networking sites is not allowed.
  - Posting of pupil images should only be under the guidance of a member of staff and in no circumstance with the pupil's full name.
  - Pupils' irresponsible use of the internet will result in temporary/permanent exclusion of use.

Members of staff are reminded that they should not deliberately seek out inappropriate/offensive materials on the Internet and that they are subject to the LA's recommended disciplinary procedures should they do so.

Child's name _____ and signature _____

Signed _____ date _____
(parent/guardian)

Approved _____ date _____
(Head/class teacher)

Stokes Wood Primary School

Pupils - Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning.

These rules will keep everyone safe and help us be fair to others.

- **I will use only my own login and password, which I will keep secret.**
- **I will not access other people's files.**
- **I will use the computers only for schoolwork and homework.**
- **I will ask permission from a member of staff before using the Internet.**
- **The messages I send will be polite and sensible; I will not send messages electronically using abusive, inappropriate or unkind comments.**
- **I will not give my home address or phone number, or arrange to meet someone, unless my parent has given permission.**
- **I will not give out personal contact details on line or post photographs of myself on sites.**
- **To help protect other pupils and myself, I will tell a teacher or other adult if I see anything I am unhappy with or I receive a message I do not like; I will not respond to abusive emails.**
- **I understand that the school can check my computer files and the Internet sites I visit.**

Stokes Wood Primary School Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's online policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, email, digital cameras, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the online Co-ordinator/the Designated Child Protection Co-ordinator/Headteacher.
- I will ensure that electronic communications with parents, carers and pupils are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will not use social media sites in school and will not communicate with pupils, parents or carers via social networking sites.
- I will not discuss school issues, incidents, business, pupils, colleagues or anything else concerning my work in school on social media.
- I will promote online with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: …… Print name: …… Date: ……

Accepted for school: Signed …… Print name: ……

Appendix 2 – Acceptable and Unacceptable User Actions

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008.					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986.					X
	Pornography				X	
	Promotion of any kind of discrimination.				X	
	Threatening behaviour, including promotion of physical violence or mental harm.				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.				X	
Using school systems to run a private business.					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy.					X	

Infringing copyright					X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords).					X
Creating or propagating computer viruses or other harmful files.					X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet).				X	
Online gaming (educational e.g. Interlard)		X			
Online gaming (non-educational)				X	
Online gambling				X	
Online shopping / commerce			X		
File sharing via School IT Systems			X		
Use of social media			X		
Use of social media to message stakeholders				X	
Use of messaging using communication apps e.g. outlook and TEAMs	X				
Use of video broadcasting e.g. YouTube		X			

Appendix 3 – Reporting Pupil Incidents

Pupils

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

Appendix 4 – Staff Concerns Flow Chart