Stoke by Nayland C of E Primary School

St Edmundsbury and Ipswich
Diocesan Multi Academy Trust

Online Safety Policy

Approved by:	*Local Governing Body*
Date approved:	*Jane 2024*
Review date:	*Summer 2025*

Online Safety Policy Principles

At Stoke by Nayland C of E Primary School we recognise that Internet use is an essential part of education at school and for the future prospects of our pupils. The speed with which the Internet and access to it develops makes it imperative that our children are in the best possible position to take advantage of its merits but, also to be aware and able to cope with problems that may arise, particularly in regard to safeguarding.

The school believes that Online Safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles and, identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of our School's Online Safety Policy is to:

- Clearly identify the key principles expected of all members of the school community with regards to the safe and responsible use of technology to ensure that our school is a safe and secure environment.
- Safeguard and protect all members of our school community online.
- Raise awareness with all members of our school community regarding the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This Policy applies to all staff including teachers, support staff, the Local Governing Body, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this Policy) as well as children and parents/carers.

This Policy applies to all access to the Internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with School issued devices for use off-site, such as work laptops, tablets or mobile phones.

Vision

Stoke by Nayland C of E Primary School is a caring, Church of England school, whose values are built firmly on a Christian foundation. We have an expectation that children and adults will behave with mutual respect and kindness towards one another and engender a trust that will lead to positive relationships. We also believe that children need to take responsibility for their behaviour and the choices they make.

The school's Online Safety Policy reflects our **Christian vision**:

As a church school our school vision is deeply rooted in Christian narrative, the story of the Good Shepherd (John 10) and the Parable of The Lost Sheep (Luke 15, Matthew 18). The story encapsulates perfectly what we think is special about our school – just as the Shepherd gives his all to secure the safety of every last sheep and helps them to thrive, so our staff give their all to create a safe and loving environment for every child so that they can be the best that they can be. We prepare our children to go out into the world equipped with everything that is good for the good of all. We are an inclusive school, welcoming all children with respect, understanding and dignity. We have a duty of care to

the children and will demonstrate the compassion and understanding that allows all children and adults within our school family and local community to flourish. In the context of this policy, this means that we aim to provide a safe and secure environment, in which children's individual needs are catered for and supported. It also means that we endeavour to provide children with the knowledge and skills they need to keep themselves safe. We recognise the moral and statutory responsibility placed on all staff to safeguard and promote the welfare of all children.

'**May the God of peace.. that great Shepherd of sheep, equip you with everything good for doing his will' Hebrews 13:20-21**

At Stoke by Nayland, we educate the whole child - their heart and mind. Our children become learners for life through the rich curriculum we provide that builds on the talents of every individual to ensure they reach their full potential, as God intended. Our children will be the best that they can be, reaching their full potential academically, socially, emotionally and spiritually. At Stoke by Nayland, we know that learning takes patience, courage and resilience. We know that learning is a journey and that all of us make mistakes as part of that journey.

We recognise that our children are individuals and sometimes need a personalised approach to enable them to experience success. We know that children thrive academically when they feel safe and secure. We base all our learning on our school values of ***Love, Courage, Compassion and Truth.***

Aims:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The Designated Safeguarding Lead (DSL) is Mrs Kelly McGrath (Headteacher)

The Online Safety lead for the Local Governing Body is Mr Will Akast

The Local Governing Body will review this Policy and its implementation at least annually or sooner if required.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

Local Governing Body
The Local Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governor with responsibility for monitoring Online Safety will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Computing Coordinator:

- Developing, and owning the Online Safety vision and culture and promoting it to all stakeholders, in line with national and local recommendations, with appropriate support and consultation throughout the school community.
- Ensuring that Online Safety is viewed by the whole community as a safeguarding issue and proactively developing a robust Online Safety culture.
- Ensuring that suitable and appropriate filtering and monitoring systems are in place, which are updated on a regular basis, to protect children from inappropriate content and contact online, that meet the needs of the school community whilst ensuring children have access to required educational material.
- Supporting technical staff in monitoring the safety and security of school ICT systems and networks and to ensure that the school network system is actively monitored and protected against viruses and malware.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding Online Safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that Online Safety is embedded within a progressive whole school curriculum that enables all pupils to develop an age-appropriate understanding of Online Safety and the associated risks and safe behaviours.
- Being aware of any Online Safety incidents and ensuring that the DSL is informed and that they are reported upon.
- Ensuring there are robust reporting channels for the school community to access regarding Online Safety concerns, including internal, local and national support.
- Ensuring that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- Auditing and evaluating current Online Safety practice to identify strengths and areas for improvement.

Designated Safeguarding Lead:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Acting as a named point of contact for all online safeguarding issues and incidents, liaising with other members of staff and other agencies as appropriate.
- Ensuring that any online safety incidents are logged (see appendices) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged (on CPOMS) and dealt with appropriately in line with the school Behaviour Policy.
- Ensuring that Online Safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Working with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Monitoring the school's Online Safety incidents to identify gaps/trends and use this data to update the school's education response to reflect need
- Reporting to the Local Governing Body and other agencies as appropriate, on online safety concerns.
- Working with the Local Governing Body to review and update the Online Safety Policy, Acceptable Use Policy (AUP) and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensuring that Online Safety is integrated with other appropriate school policies and procedures.

All staff members:

- Maintaining an understanding of this policy and implementing it consistently.
- Contributing to the development of the Online Safety policy.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use Reading the School Acceptable Use Policy.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy.
- Embedding Online Safety education in curriculum delivery wherever possible.

Children:

- Contributing to the development of the Online Safety Policy.
- Reading (with their parents as necessary), the school Acceptable Use Policy (AUP) and adhering to it.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing Online Safety issues.
- Taking responsibility for keeping themselves and others safe online.

Parents and carers:

- Reading the school Acceptable Use Policy, encouraging their children to adhere to it, and adhering to it themselves where appropriate.
- Discussing Online Safety issues with their children, supporting the school in their Online Safety approaches, and reinforcing appropriate safe online behaviours at home.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school Online Safety policy.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety may also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher (DSL) or the Deputy DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7. Acceptable use of the Internet in school

All pupils, parents, staff, volunteers, visitors (where appropriate) and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the Internet . Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's Internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in school

- Pupils are not permitted to bring mobile phones or communication devices into school unless approved in advance by the Headteacher. If pupils are found to have such a device it will be confiscated and placed in the School Office until the end of day.
- If a pupil needs to contact his/her parents/carers they will be allowed, if the circumstances warrant it, to use a school phone or a staff member will make the call on their behalf.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendices.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work

device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Computing Coordinator.

Work devices must be used solely for work activities.

Staff are not permitted to use personal phones to take photos of the children.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT 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.

Where a staff member misuses the school's ICT systems or the Internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

The DSL and deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe Internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the Local Governing Body.

13. Links with other policies

This Online Safety Policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-bullying Policy
- Acceptable Use of IT Policy
- ICT Policy

- Data Protection Policy
- Complaints Procedure
- Whistleblowing Policy

13. Online Communication and Safer Use of Technology

13.1 Managing the School website

- The Headteacher and Computing Leader will take overall editorial responsibility for online content published.
- Pupils' images will only be published with the permission of their parents/carers. Pupils' full names will not appear.

13.2 Managing email

- Pupils may only use school provided email accounts for educational purposes.
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff to communicate personal data is not permitted.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school's safeguarding files/records.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission from a member of staff. This would be only as a pre-planned activity that supports schoolwork and with parental knowledge
- Whole-class or group email addresses, if provided, may be used for communication outside of the school.
- School email addresses will not be used for setting up personal social media accounts or used for personal reasons.

13.3 Appropriate and safe classroom use of the Internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age, maturity and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- The school's Internet access will be designed to enhance and extend education.
- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.
    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and

approved online materials which supports the learning outcomes planned for the pupils' age and ability.

- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources that support the learning outcomes planned for the pupils' age and ability.

- All school-owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. They will also be told what constitutes unacceptable use.
- The school will use age appropriate search tools (search tools suggested for staff and pupils to use such as SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search) as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

14. Social Media Policy

14.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of our school community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of our school community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of our school community.
- All members of our school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.
- The use of social networking applications by pupils during school hours for personal use is not permitted. Staff access is allowed during official breaks.
- Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the Headteacher and will be managed in accordance with School policy.
- Any breaches of School policy may result in criminal, disciplinary or civil action being taken.
-

14.2 Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the Headteacher.
- If on-going contact with pupils is required once they have left the school roll, then members of staff will be expected to use official School provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels where possible, such as school email address. Staff personal mobile phones are sometimes used where necessary (e.g. texts to parents with hearing difficulties), until the school's telephone system is upgraded.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, unless the Headteacher gives prior approval.
- Any communication from pupils/parents received on personal social media accounts will be reported to the Headteacher.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies (Safeguarding, Data Protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Headteacher immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.
- Members of staff are encouraged not to identify themselves as employees of the school on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as those of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.

14.3 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will inform the Headteacher of any concerns such as criticism or inappropriate content posted online.

15. Use of Personal Devices and Mobile Phones

15.1 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies (AUP).
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Behaviour Policy.
- Members of staff will be issued with a work email address where contact with pupils or parents/carers is required. The school main telephone number should be used for phone contact.
- All members of the school community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of staff will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential.
- All members of staff will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene school policies.
- School devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
- School devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

15.2 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children and their families within or outside of the setting in a professional capacity (unless there are exceptional circumstances). In the majority of cases, staff are expected to use the school's landline. There are exceptional circumstances mentioned earlier in this Policy and this would include out of school activities where the staff member needs to contact a parent, for example to request permission to give medication to a pupil, in such cases, the number should be withheld. It is appreciated that, as the school does not issue school-owned mobile phones, there may be occasions when the Headteacher or Senior Teacher may need to use their personal mobiles to contact parents, but whenever possible, the school's landline should be used. Any pre-existing relationships that could compromise this will be discussed with the Headteacher.

- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose, unless permitted by the Headteacher.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times and placed out of sight, unless there are exceptional circumstances which have been agreed in advance with the Headteacher.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by the Headteacher.

15.3 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's Acceptable Use Policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with School policy.
- The school will ensure information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Headteacher of any breaches of use by visitors.

16. Managing Information Systems

16.1 Filtering and Monitoring

- The school uses educational filtered secure broadband connectivity subscribed through Schools Choice that is appropriate to the age and requirement of our pupils.
- The school uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school uses secures – which identifies at risk words and the device they have been searched from or used on
- The school will work with Schools' Choice and the school's IT support or broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Police or CEOP and SCC immediately.

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- The school views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Headteacher.
- The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people'

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- The school will ensure that all members of the community are made aware of online child sexual abuse, child exploitation and grooming, including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Headteacher as Designated Safeguarding Lead.

Responding to concerns regarding Indecent Images of Children (IIOC)

- The school will ensure that all members of the school community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.

Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the Internet in school and that suitable filtering is in place that takes into account the needs of pupils.
- If staff are concerned that a child may be at risk of radicalisation online, the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the Safeguarding Policy.
- Online hate content directed towards or posted by specific members of the school community will be responded to in line with existing School policies, including Anti-bullying, Behaviour etc.

Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the school community will not be tolerated. Full details are set out in School policies regarding Anti-bullying and Behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

Responding to concerns regarding online hate

- Online hate at the school will not be tolerated. Further details are set out in School policies regarding Anti-bullying, Equality and Behaviour.
- All members of the school community will be advised to report online hate in accordance with relevant School policies and procedures e.g. Anti-bullying, Behaviour etc. and all incidents will be recorded.

Online-Safety Incident Report
Stoke by Nayland C of E Primary School

Your Details	Your Name:	Your Position:

Date and Time of Incident:

Where did the incident occur? i.e.: School or home

Who was involved in the incident?

Child/Young person: Y/N

Name of Child/ren:

Staff Member/Volunteer: Y/N

Name of staff member/volunteer:

Other

Please Specify:

Description of incident: (Include as much detail as possible including user names, devices programmes used)

Action Taken:

Incident reported to Headteacher/Senior Teacher

Advice sought from Safeguarding and Social Care

Referral made to Safeguarding and Social Care

Incident reported to the Police

Incident reported to Internet Watch Foundation

Disciplinary action to be taken

Online Safety Policy to be reviewed/amended **Other – (Please specify) ……..**
Outcome of investigation: