St Edmundsbury and Ipswich Diocesan Multi Academy Trust

Stoke by Nayland C of E Primary School
Acceptable Use of ICT Policy

The aims of this Acceptable Use of ICT Policy are to:

- Ensure that all pupils benefit from the learning opportunities offered by the Internet resources provided by the school, in a safe and controlled manner.
- Ensure that all staff benefit from Internet access, with clear guidance on safe and acceptable use.
- Protect against accidental or deliberate misuse.
- Make staff and pupils aware that Internet use in school is both a resource and a privilege. If the terms of use are not met, the use of ICT will be restricted.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and personal items that may be brought into school.

This policy should be read in conjunction with the Online Safety Policy

1. General

1.1 Virus protection software is used and updated on a regular basis.
1.2 A member of staff is appointed as responsible for the school's Online Safety.
1.3 Stoke by Nayland C of E Primary School contracts with Design Communication (UK) Limited for its broadband service, using a Meraki firewall.

2. School Responsibilities

2.1 The Local Governing Body is responsible for ensuring that employees act in a lawful manner, making appropriate use of school technologies for approved purposes.
2.2 The Local Governing Body is responsible for adopting the relevant policies and the Headteacher for ensuring that staff are aware of their contents.
2.3 The computing coordinator is responsible for maintaining an inventory of equipment and to whom equipment is issued.
2.4 If staff members wish to borrow ICT equipment for school work at home, the computing coordinator should record the loan and complete an Equipment Loan Form in accordance with school policy.
2.5 If the Headteacher has reason to believe that ICT equipment is being used inappropriately, or in a way that may compromise safeguarding or safer recruitment practises, they will report such actions to the relevant authorities.

3. Pupil Access to the Internet

All staff at Stoke by Nayland C of E Primary School take the issue of safeguarding very seriously. If an adult has reason to believe that a child is at risk from the use of the Internet, they will follow the safeguarding procedures (see Child Protection and Safeguarding Policy)

3.1 Members of staff are aware of the potential for misuse, and will be responsible for educating and explaining to pupils, the expectations we have.
3.2 Our school environment is such that the ICT suite is within easy reach of staff who will intervene if necessary.
3.3 Teachers will have access to pupils' ICT related files and will check these as necessary on a regular basis to ensure expectations of behaviour and use are being met.

4. Expectations of Pupils using the Internet and other ICT Resources

4.1 All pupils are expected to read and agree the Acceptable Use Agreement.

4.2 We expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

4.3 Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any pupil encounter any such material accidentally, they are expected to report it immediately to a teacher, so that further access to the site can be blocked.

4.4 Pupils are expected to use acceptable language; any rude language found in ICT files will result in restricted access. Pupils may only communicate and contact people they know or those the teacher has approved. They have been taught the rules of etiquette for email.

4.5 Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.

4.6 Pupils should not access other people's files unless permission has been given.

4.7 Computers should only be used for schoolwork and homework unless permission has been granted by a teacher or adult otherwise.

4.8 No program files or applications may be downloaded to computers from the Internet. This is to prevent corruption of data and avoid virus infection.

4.9 Pupils should not bring in memory sticks or other data media from home to use at school unless a teacher has given approval. This is for both legal and security reasons. However, on occasions, homework may be brought in on a memory stick, but this will have to be agreed in advance and the media virus scanned by the class teacher before use.

4.10 Personal information such as phone numbers and addresses should not be given out and no arrangements to meet someone made unless this is part of an approved school project.

4.11 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.

4.12 Other ICT devices may only be brought in from home, with the prior permission of the Headteacher or computing coordinator. Inappropriate use is a breach of this Acceptable Use Policy.

(A children's version of ICT responsibilities is included in the appendices)

Stoke by Nayland C of E Primary School is a Safer Recruitment School

5. Expectation of Adults Using the Internet

All adults working in School in employment, in a voluntary capacity or using the community Internet site are expected to broadly abide by the standards set for pupils.

Additionally:

5.1 They are expected to protect passwords and not share school or pupil, or personal data with those without an entitlement to see it.

5.2 They must take care of sensitive data relating to pupils or staff or parents in compliance with the GDPR and data protection legislation.

5.3 ICT may not be used to transmit threatening material, chain letters or spam, or material of a violent or sexual nature, or of a discriminatory nature *(see Equality Policy).*

5.4 If a member of staff suspects that these terms are being breached, they should refer to the "Whistleblowing Policy" and report the matter to the Headteacher.

The school may record or inspect any information transmitted through or stored in its computers without notice when it suspects there is reasonable cause to believe that a user has violated the terms of this Policy.

6. Social Networking

The school recognises that staff may wish to actively use Facebook, Twitter, Instagram and other such social networking sites. To protect the reputation of staff and the school they must not post material (including text or images) which may damage the reputation of the school or which causes concern about their suitability to work with children. Staff must not talk about school matters or their professional role in any capacity via these networks.

6.1 Any online safety incident which may have an impact on you, your professionalism or the school should be reported to the Headteacher. If in doubt, this should be discussed with the Headteacher.

6.2 If a member of staff suspects that these terms are being breached, they should refer to the 'Whistleblowing Policy' and report the matter to the Headteacher.

7. School Website / Social Media Page

7.1 The website and social media page will be regularly checked to ensure that the content does not compromise the safety of pupils or staff.

7.2 The publication of a child's work will be decided by a teacher and only children's first names will be recorded.

7.3 The school will not use digital photographs or video clips without parental consent, (unless it is a group activity photograph which cannot identify individuals).

7.4 The school will ensure that the image files are appropriately named and will not use pupils' names in image file names, if published on the internet.

8. Applying our Acceptable Use Policy (AUP)

We aim to give users every opportunity to use ICT as a valuable educational and fun source of learning. However, persistent and deliberate misuse of the internet and other ICT equipment by pupils will result in access being reduced to when activities can be closely monitored. This sanction will be for a set time according to the age of the pupil and the nature of the misuse and, be in line with our Behaviour Policy. Parents will be informed of any serious breaches of policy by their child.

Date: *July 2021* *Review:* Annually

Appendix 1

Stoke by Nayland C of E Primary School

Home/School ICT and Internet Agreement for Early Years and KS1 Pupils

Please read this form with your child to help them understand that it is important to use ICT sensibly and safely

- I will always take care and look after computers, tablets and other ICT equipment
- I will only use the internet when an adult is with me
- I will only click on links and buttons when I know what they do
- I will keep my personal information and passwords safe and I will not share my passwords with friends
- I will not let anyone know my full name, address or telephone number on the Internet
- I will not download any files from the Internet without permission from a teacher / adult
- I will only print from the Internet in school with permission
- I only send messages online which are polite and friendly and I do not use rude words
- I will not go into anyone else's file without permission
- I know the school can see what I am doing online
- I will always tell an adult/teacher if something online makes me feel unhappy or worried
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online

I have read through this home/school safe use of ICT agreement with my child and agree to these safety restrictions.

Signed: …….. (*Parent / Carer)*

Child's name: …….. *(Print)*

Signed: ……..…. *(Child, if you feel they are old enough to sign)*
Please keep one copy and return the other to School

Appendix 2

Stoke by Nayland C of E Primary School

Home/School ICT and Internet Agreement for KS2 Pupils

Please read this form with your child to help them understand that it is important to use ICT sensibly and safely

- I will behave sensibly and responsibly when using the Internet and ICT equipment
- I always ask permission from an adult before using the Internet
- I only use websites and search engines that my teacher has chosen
- I only click on links and buttons when I know what they do
- I only talk with and open messages from people I know and I only click on links if I know they are safe
- I keep my personal information and passwords safe online and I will not share my passwords with friends
- I will not let anyone know my full name, address or telephone number on the Internet or arrange to meet someone I do not know
- I will not download any files from the Internet without permission from a teacher / adult
- I will not look for bad language, inappropriate images or violent or unsuitable games and, if I accidentally find any of these I will report this to a teacher or adult in school or my parent / carer at home
- I will not print anything from the Internet in school without permission
- I only send messages online which are polite and friendly
- I will not go into anyone else's file without permission
- I will not transfer any games or programmes to school computers. If I want to use a memory stick on a school computer I will ask the teacher's permission, to make sure the media is not infected with a virus and is appropriate
- I know the school can see what I am doing online
- I always tell an adult/teacher if something online makes me feel unhappy or worried
- I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use
- I will only change the settings on the computer if a teacher has allowed me to
- I understand that the school's internet filter is there to protect me
- I know that if I do not follow the rules then I may not be allowed full use of the Internet in school
- I know that I am not allowed to have a mobile phone or my own tablet in school, if I need to bring these to school they must be handed-in to the School Office and collected at the end of the school day
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online

I have read through this home/school safe use of ICT agreement with my child and agree to these safety restrictions.

Signed: …….. (*Parent / Carer)*

Child's name: …….. *(Print)*

Signed: ……..…. *(Child, if you feel they are old enough to sign)*

Please keep one copy and return the other to school

Appendix 3

Stoke by Nayland C of E Primary School

ICT and Internet Staff Acceptable Use Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the School's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the School's ethos, other appropriate School policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School-owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.

5. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).

6. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system administrator.

7. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018 and General Data Protection Regulations. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data that is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and, will always take into account parental consent.

8. I will not keep or access professional documents that contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. I will protect the devices in my care from unapproved access or theft and ensure that nobody is able to view my screen when I am looking at personal data, unless they are authorised to do so.

9. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

10. I will respect copyright and intellectual property rights.

11. I have read and understood the school Online Safety Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

12. I will report all incidents of concern regarding children's Online Safety to the Designated Safeguarding Lead (Headteacher) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead as soon as possible.

13. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the Computing Coordinator as soon as possible.

14. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email or social networking. Any pre-existing relationships or situations that may compromise this will be discussed with the Headteacher. Office staff may use personal mobiles for texting parents/carers with hearing difficulties until alternative arrangements are made.

15. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and the Internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

16. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the School, or St Edmundsbury and Ipswich Diocesan Multi Academy Trust into disrepute.

17. I will promote Online Safety with the pupils in my care (if applicable) and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

18. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Headteacher).

19. I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

The school may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the school's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: ……..

Print Name: …… Date: ……

Accepted by: …….. Print Name: ……

Appendix 4

Stoke by Nayland C of E Primary School

ICT and Internet Visitor/Volunteer Acceptable Use Policy

For visitors/volunteers and staff who do not access School ICT systems

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school's ethos, other appropriate School policies, relevant national and local guidance and expectations, and the Law.

1. I have read and understood the School Online Safety Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

2. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

3. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Headteacher.

4. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law

5. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or St Edmundsbury and Ipswich Diocesan Multi Academy Trust, into disrepute.

6. I will promote Online Safety with the children in my care (if any) and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

7. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Headteacher).

8. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible.

I have read and understood and agree to comply with the Visitor /Volunteer Acceptable Use Policy.

Signed: ……..... Print Name: ……..

Date: ……

Accepted by: …… Date: ……...

Stoke by Nayland C of E Primary School

Wi-Fi Acceptable Use Policy

For those using school Wi-Fi

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school's boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the School's ethos, other appropriate policies and the Law.

Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the school.

The school may provide Wi-Fi access to the Internet in exceptional circumstances, approved by the Headteacher or the ICT Coordinator.

1. The use of ICT devices falls under Stoke by Nayland C of E Primary School's Acceptable Use Policy, Online Safety Policy and Behaviour Policy, which all pupils/staff/visitors and volunteers must agree to, and comply with.

2. The School reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

3. School-owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

4. I will take all practical steps necessary to make sure that any equipment connected to the school's service is adequately secure (such as up-to-date anti-virus software, systems updates).

5. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

6. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

7. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

9. I will not attempt to bypass any of the school's security and filtering systems or download any unauthorised software or applications.

10. My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

11. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

12. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Headteacher), or the ICT Coordinator as soon as possible.

13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Computing Coordinator or the Headteacher.

14. I understand that my use of the school's Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school will terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with Stoke by Nayland C of E Primary School Wi-Fi Acceptable Use Policy.

Signed: ……..... Print Name: …….

Date: ……

Accepted by: ……. Print Name: …….