All Saints Schools Trust

Online Safety Policy

1. Creating an Online Safety Ethos

1.1 Aims and Policy Scope

- All Saints Schools Trust believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers and tablets, mobile phones or games consoles.
- All Saints Schools Trust identifies that the internet and information communication technologies are now an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk in order that they are empowered to build resilience online.
- All Saints Schools Trust has a duty to provide school communities with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the schools' management functions. All Saints Schools Trust also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.
- The purpose of All Saints Schools Trust online safety policy is to:
    - Clearly identify the key principles expected of all members of the All Saints Schools Trust community with regards to the safe and responsible use of technology to ensure that All Saints Schools Trust is a safe and secure environment.
    - Safeguard and protect all members of the All Saints Schools Trust community online.
    - Raise awareness with all members of the All Saints Schools Trust community regarding the potential risks alongside the benefits of technology.
    - To enable all staff to work safely and responsibly, to role 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 All Saints Schools Trust staff including the Trustees, Members, Governing Bodies, all teaching and other staff, 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 individual have been provided with school issued devices for off-site use, such as a work laptop or mobile phone.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, behaviour,

data security, image use, Acceptable Use Policy, and relevant curriculum policies.

1.2 Writing and Reviewing the Online Safety Policy

- All Saints Schools Trust's online safety policy has been written by school leaders, involving staff, pupils and parents/carers.
- The Trust's policy has been approved and agreed by the Leadership Team and governing body.
- The Trust has appointed members of school Governing Bodies to take lead responsibility for online safety.
- The Trust has appointed a members of the leadership team as the Online Safety Lead in each school.
- The Trust's Online Safety Policy and its implementation will be reviewed at least annually or sooner if required.

1.3 Key Responsibilities of the School Community

1.3.1 Key responsibilities of the school management team

The key responsibilities of the school management team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Support the online safety lead in the development of an online safety culture within the setting.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs to the school community and ensuring that the filtering and school network system is actively monitored.
- 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 which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of the school's systems and networks.
- To ensure that the DSL works in partnership with the online safety lead (if they are not the same person).

1.3.2 Key responsibilities of the designated safeguarding/online safety lead

The key responsibilities of the designated safeguarding/ online safety lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour (e.g. Safer Internet Day).
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the setting lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident log to record incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- Monitor the school's online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 Key responsibilities of all staff

The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school's Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of the school's systems and data.
- Having an awareness of the online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery where possible.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead (DSL).
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both within and outside school.

1.3.4 Additional responsibilities for staff managing the technical environment

In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support online safe practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership team.
- To ensure that suitable access controls/ encryption are implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
- Ensuring that the use of the school's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- To report any breaches or concerns to the DSL and leadership team, ensuring they are recorded in the Online Safety Incident Log, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- To report any breaches security in the school's network and to liaise with the local authority (LA) as appropriate on technical infrastructure issues.
- To provide technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on school machines and portable devices.

1.3.5 Key responsibilities of children and young people

The key responsibilities of children and young people are:

- Contributing to the development of online safety policies (so that they feel a sense of ownership and can share their knowledge of latest advances and trends in technologies.)
- Reading and adhering to the school's Acceptable Use Policy (AUP).
- 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.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 Key responsibilities of parents and carers

The key responsibilities of parents and carers are:

- Reading the school's Acceptable Use Policies (AUPs), encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approach and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- 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 encounter online problems or concerns.

2. Online Communication and Safer Use of Technology

2.1 Managing the school's website

- The school will ensure that the information posted on the school website meets the requirements identified by the Department for Education.
- The contact details on the website will be the school's address, email and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- The school will post information about safeguarding, including online safety, on school website.

2.2 Publishing images and videos online

- The school will ensure that all images are used in accordance with the school image use policy.
- In line with the school's image policy, written permission from parents and carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing Email

- As far as possible school email accounts will be set up.
- Any referrals being sent to outside agencies will go via secure school email accounts.

2.4 Appropriate Safe Classroom Use of the Internet and Associated Devices

- 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.
- Pupils will use age and ability appropriate tools to research Internet Content (See separate planning – whole school online safety approach. Appendix 1)
- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum (Appendix 1).
- 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.
- 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 internet use is essential.
- At EYFS and KS1, 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 KS2, 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 materials and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Pupils will be educated in an age-appropriate way on how to use the internet and all related devices in a safe and responsible way.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

- 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.
- Members of staff will always evaluate websites, tools and apps before use in the classroom or recommending for use at home.

3. Social Media Policy

3.1 General Social Media Use

- Expectations regarding safe and responsible use of social media will apply to all members of All Saints Schools Trust 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, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of All Saints Schools Trust 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 All Saints Schools Trust community.
- All members of All Saints Schools Trust's 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 pupils and staff access to social media and social networking sites whilst on site and using school provided devices and systems.
- The use of social networking applications during school hours for personal use is not permitted (unless it is during a lesson and explicit permission has been given by the class teacher after discussion and agreement by DSL/ Senior Leaders.)
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of All Saints Schools Trust community on social media sites should be reported to the school leadership team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken. This will depend upon the age of those involved and the

circumstances of the wrong committed. Action taken will be in accordance with the relevant school policies (such as anti-bullying, allegations against staff, behaviour and safeguarding/ child protection).

3.2 Staff Personal Use of Social Media

- Personal 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 staff (including volunteers) as part of the school Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social mediate sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the Headteacher / member of the Senior Leadership Team. If ongoing contact with pupils is required once they have left the school roll, then staff will be expected to use existing alumni networks or use official school communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels. Staff must not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils/parents received on personal social media accounts will be reported to the school's DSL.
- Information 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 the 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 post online and ensure that their social media use is compatible with their professional role and is in accordance with the school's policies (safeguarding, confidentiality, data protection etc.) and wider legal framework.
- Members of staff will be encouraged to manage and control the content they post online and advice will be provided to staff via training and by sharing appropriate guidance and resource on a regular basis.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content 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 Stradbroke Primary 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 school community.

3.5 Pupils' Use of Social Media

- Personal publishing on social media sites will be taught to pupils via the computing and PSHE curriculum as part of an embedded and progressive education approach (See Appendix 1)
- Safe Social Media skills will be taught to pupils via age appropriate sites that have been risk assessed and approved as suitable for educational purposes.
- The School is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age.
- Parents will be informed of any official social media use with pupils and official activity will be moderated by the school where possible.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be dealt with in accordance with existing school policies and will be raised with their parents/carers, particularly when concerning any underage use of sites.
- Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the school's Acceptable Use Policy.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and strong passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding Personal Devices and Mobile Phones

- The widespread ownership of mobile phones and a range of other personal devices among young people and adults will require all members of the community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults in school will be decided by the school and covered in appropriate policies.
- The school recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for Safe Use of Personal Devices and Mobile Phones

- Electronic devices of all kinds that are brought in to school 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.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

4.3 Children's Use of Personal Devices and Mobile Phones

- Use of mobile phones and personal devices by children will take place in accordance with the school Acceptable Use Policy (AUP).
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are not permitted to contact their child via a mobile phone during the day, but are to contact the school office.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile

phones and devices will be released to parents/carers at the end of the school day as appropriate.

- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or device may be searched by the Senior Leadership team with consent of the pupil or parent/carer. If there is suspicion that the material on the mobile phone or personal device may be illegal or may provide evidence relating to a criminal offence, it will be handed over to the police for further investigation.

4.4 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, young people and their families within or outside of the setting unless in a professional capacity. Any pre-existing relationships which compromise this must be discussed with leaders/managers.
- 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.
- Staff personal mobile phones and devices will be switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be 'hidden' or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Leadership Team.
- Staff will ensure that any content brought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the policy, then disciplinary action will be taken. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted and allegations will be responding to following the school's allegations management policy.

4.5 Visitors' use of Personal Devices and Mobile Phones

- Parents/carers and visitors must use mobile phones or personal devices in accordance with the school's policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos of videos must take place in accordance with the school's image use policy.

5. Policy Decisions

5.1 Reducing Online Risks

- All Saints Schools Trust is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for education benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.
- The school will take all reasonable precautions to ensure that users only access appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

5.2 Internet use within the school community

- The school will be sensitive to Internet-related issues experience by pupils out of school (e.g. social networking sites) and offer appropriate advice.
- The school will provide an AUP for any guest/visitor who needs to access the school computer system or internet on site.

5.3 Authorising Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff, pupils and visitors will read and sign the school's AUP before using any school ICT resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the school's AUP for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the school community (such as children with SEN), the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible Internet use amongst pupils.
- Education about safe and responsible use will precede Internet access.
- Pupils' input will be sought when writing and developing school online safety policies and practices.
- Pupils will be supported in reading and understanding the school's AUP in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety will be included in the PSHE and Computing programmes of study covering both safe school and home use.
- Online safety education and training will be included as part of the transition across that Key Stages, including between establishments.
- The pupil AUP will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement the school's internet online safety education approaches.
- Particular attention to differentiated online safety education will be given where pupils are considered to be vulnerable, with input from specialist staff (e.g. SENCO) as appropriate.
- The school will endeavour to implement peer education to develop online safety as appropriate to the needs of the pupils.

6.2 Engagement and education of staff

- The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of the school's safeguarding practice.
- To protect all staff and pupils, the school will implement AUPs which highlight appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputations within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.3 Engagement and education of parents and carers

- All Saints Schools Trust recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school Online Safety Policy and expectations in newsletters, letters, and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations for safe home Internet use.
- Parents will be requested to read Online Safety information as part of the Home School Agreement.
- Parents will be encouraged to read the AUP for pupils and discuss its implications with their children.
- Information and guidance for parents about Online Safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Responding to Online Incidents and Concerns

- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Online Safety Lead will record all reported incidents and actions taken in the School's online safety incident log and in any other relevant areas (e.g. bullying or child protection log).
- The DSL will be informed of any online safety incidents involving child protection concerns, which will then be escalated and reported to the relevant agencies in line with the Suffolk Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online bullying will be dealt with under the School's anti-bullying policy.
- Any complaint about staff misuse will be referred to the Headteacher.
- Any allegations against a member of staff's online conduct will be discussed with LADO (Local Authority Designated Officer – LADOCentral@suffolk.gcsx.gov.uk or 0300 123 2044)
- Pupils and parents will be informed of the complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which may cause harm, distress or offence to any other members of the school community.
- The school will manage online safety incidents in accordance with the school's discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concern as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Suffolk Safeguarding Childrens' Board and escalate the concern to the Police via 101 or 999 if there is immediate danger.
- The use of computer systems without permission of for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Suffolk Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the LADO.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Online Safety Officer to communicate to another school in Suffolk.
- Parents and pupils will need to work in partnership with the school to resolve issues.

8. Managing Information Systems

8.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Full information regarding the school's approach to data protection and information governance can be found in the school's information security policy.

8.2 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Files held on the school's network will regularly be checked.
- The network manager will review system capacity regularly.

8.3 Filtering Decisions and Online Safety

- The Trust uses educational filtered secured broadband connectivity through Suffolk County Council (SCC) which is appropriate to the age and maturity of pupils.
- The school uses E2BN Protex Web Filtering systems which block sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school will ensure that suitable filtering is in place whilst using school devices and systems to try and prevent staff and pupils from accidentally or deliberately being exposed to unsuitable content.
- The school will work with SCC to ensure that the filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the DSL and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites in line with the Internet Watch Foundation (IFW) list.
- The SLT 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 the appropriate agencies such as Suffolk Police or CEOP immediately.

Appendix:

1. Parent AUP
2. Letter to accompany Parents AUP
3. Staff AUP
4. Letter to accompany Staff AUP
5. Pupil AUPs
6. Visitor Volunteer AUP
7. Wi-fi Acceptable Use

Appendix 1- Parent/ Carer AUP

Parent/Carers Acceptable Use Policy

- I have read and discussed the Children's Acceptable Use Policy (attached) with my child.
- I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet and the school is not liable for any damages arising from the use of Internet facilities.
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted.
- I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the school's behaviour and anti-bullying policy. If the school believes that my child has committed a criminal offence, then the Police will be contacted.
- I, together with my child, will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of, offend or defame any member of the school community or the school itself.
- I know that I can speak to the Online Safety Lead, my child's teacher or the Head Teacher if I have any concerns about online safety.
- I will visit the school website for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home.
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org, www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online.
- I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

Appendix 2- Letter to accompany Parent/ Carer AUP

Dear Parent/Carer

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones

All Saints Schools Trust recognises the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed online safety policies and procedures alongside the school's safeguarding measures.

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. This includes ensuring that devices are used with appropriate supervision, use of filtering devices and a curriculum which is planned to develop children's understanding of online safety as they progress through the school. However no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the Internet and the school is not liable for any damages arising from use of the school's Internet and ICT facilities.

Full details of the school's Acceptable Use Policies and online safety policy are available on the school website or on request.

We request that all parents/carers support the schools approach to online safety by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers can visit the school website for more information about the school's approach to online safety as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online

Whilst the school monitors and manages technology use in school, we believe that children themselves have an important role in developing responsible online behaviours. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child and that you and your child discuss the content and return the attached slip. Hopefully, you

will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home. We also ask that you read the Parent/Carer Acceptable Use Policy and return the attached slip to school to confirm your agreement to follow the policy. We appreciate your cooperation with this as it is a necessary part of our Home/School Agreement.

Should you wish to discuss the matter further, please do not hesitate to contact the school Online Safety Lead and/ or Headteacher/ Head of School.

(Additional Paragraph for Early Years/KS1/SEN)

We understand that your child is too young to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

Yours sincerely,

Headteacher/ Head of School

Appendix 3- Staff AUP

Trust Staff Acceptable Use Policy

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 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 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 – include school information and requirements e.g. how often they should be changed).

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

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. 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 which 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.

7. I will not keep or access professional documents which 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. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment or via VPN. I will protect the devices in my care from unapproved access or theft.

8. 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.

9. I will respect copyright and intellectual property rights.

10. 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.

11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead and/or the Online Safety Lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead and/or the Online Safety Coordinator and/or the designated lead for filtering as soon as possible.

12. 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 ICT Support Provider/Team/lead Elliot Sheppard as soon as possible.

13. 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 Senior Leadership team and/or Head Teacher.

14. 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 internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

15. 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 the County Council, into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. 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 and/or the Head Teacher/ Head of School .

18. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service'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 system may be being used for criminal purposes or for storing unlawful text, imagery or sound, 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- Letter to accompany staff AUP

Dear Staff

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of both your professional reputation and that of the school when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, personal contact details, video or images etc online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.

If you have a social networking account, it is advised that you do not to accept pupils (past or present) or their parents/carers as "friends" on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. Please use your work provided email address or phone number to contact children and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns about this then please speak to the Online Safety Lead (Insert for each school) or Designated Safeguarding Lead (Insert for each school).

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer practise with Technology" (KENT) are available in the staffroom to help you consider how to protect yourself online. Please photocopy them if you want or download the documents directly from www.childnet.com, www.kelsi.org.uk and www.gov.uk/government/publications/preventing-and-tackling-bullying. Staff can also visit or contact the Professional Online safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school policy could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online. Please speak to your line manager, the Designated Safeguarding Lead or Headteacher if you have any queries or concerns regarding this.

Yours sincerely,

Headteacher

Appendix 5- Pupil AUPs

KS1 Acceptable Use Policy

• I only use the Internet when an adult is with me.

• I only click on links and buttons when I know what they do.

• I keep my personal information and passwords safe online.

• I only send messages online which are polite and friendly.

• I know the school can see what I'm doing online.

• I have read and talked about these rules with my parents/carers.

• I always tell an adult/teacher if something online makes me feel unhappy or worried.

KS2 Acceptable Use Policy

• I always ask permission from an adult before using the Internet.

• I only use websites and search engines that my teacher has chosen.

• I use my school computers for work unless I have permission otherwise.

• I do not bring my own personal devices (mobile phone, iPods etc.) into school unless I have asked my teacher and been given permission.

• 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 only talk with and open messages from people I know and I only click on links if I know they are safe.

• I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.

• I only send messages which are polite and friendly.

• I will keep my personal information safe and private online.

• I will keep my passwords safe and not share them with anyone (except a trusted adult in some circumstances).

• I will not access or change other people's files or information.

• I will only post pictures or videos on the Internet if they are appropriate and if I have permission.

• I understand that the school's Internet filter is there to protect me, and will not try to bypass it.

• I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

• I know what my use of school computers and Internet access will be monitored.

• If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away. If appropriate, I will report it, asking an adult to help me if I need to.

• I have read and talked about these rules with my parents/carers.

• If I am aware of anyone being unsafe with technology then I will report it to a teacher.

Appendix 6- Visitor Volunteer AUP

Visitor/Volunteer Acceptable Use Policy

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 ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. Any data which 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.

2. 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.

3. 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.

4. 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 Senior Leadership team and/or Head Teacher.

5. 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.

6. 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 the County Council, into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. 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 the Online Safety Lead or the Head Teacher.

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

I have read and understood and agree to comply with All Saints Schools Trust Visitor /Volunteer Acceptable Use Policy.

Signed: ……... Print Name: …… Date: ……

Accepted by:…… ……Date: ……..

Appendix 7- Wi-fi Acceptable Use

WiFi Acceptable Use Policy

For those using school WiFi

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 schools boundaries and requirements when using the school WiFi 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 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 provides WiFi for the school community and allows access for education use only.

1. The use of ICT devices falls under All Saints and Stradbroke Primary School's Acceptable Use Policy, online safety policy and behaviour policy and safeguarding/child protection which all students/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 WiFi, 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 schools 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 done 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 schools security and filtering systems or download any unauthorised software or applications.

10. My use of the school WiFi 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 or Headteacher/ Head of School as soon as possible.

13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Online Safety Lead/ Headteacher/ Head of School.

14. I understand that my use of the schools internet will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the schools suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school 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 All Saints Schools Trust WiFi Acceptable Use Policy.

Signed: ……... Print Name: …… Date: ……

Accepted by: …… Print Name: ……