

St John the Baptist Primary School

Online Safety Policy

Reviewed [Spring 25](#)
Gov Approved [Yes](#)
Next Review due [Spring 26](#)
Safeguarding Policies

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed). This Online Safety Policy outlines the commitment of St John the Baptist Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

St John the Baptist Primary School will deal with such incidents within this policy and associated behaviour and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This Online Safety Policy is written to protect all children and adults. At St John the Baptist Primary School we recognise that online safety encompasses not only internet technologies, but also electronic communications such as mobile phones, wireless technology, webcams and internet collaborations tools (e.g. social networking sites).

The school Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- Allocates responsibilities for the delivery of the policy
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- Describes how the school will help prepare learners to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Is supplemented by a series of related acceptable use agreements
- Is made available to staff at induction
- Is published on the school website.

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. The internet is an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT.

Online safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones, and other electronic communications technologies. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care', which applies to everyone working with children.

The school's online safety policy will operate in conjunction with other policies including those for *Behaviour*, *Anti-Bullying*, *Data Protection* and *GDPR*.

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of the community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Governors

The DfE guidance “Keeping Children Safe in Education” states: “Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare... this includes... online safety”

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the governing body whose members will receive regular information about online safety incidents and monitoring reports.

The governing body will also support school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety & Curriculum Leads

The Online Safety and Curriculum Leads will:

- Develop a planned and co-ordinated online safety education programme, using Project Evolve, which will be provided through a discrete session, PSHE and SRE sessions, assemblies and pastoral opportunities
- Work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- Take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- Have a leading role in establishing and reviewing the school online safety policies/documents
- Promote a commitment to online safety education/awareness raising across the school and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded, and evaluated
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Receive reports of online safety incidents, creating a log of incidents to inform future developments
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- Liaise with technical staff, pastoral staff and support staff
- Report regularly to headteacher/senior leadership team.

Designated Safeguarding Lead (DSL)

The DfE guidance “Keeping Children Safe in Education” states:

“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety). This should be explicit in the role holder’s job description.” ... Training should provide designated safeguarding leads with a good understanding of their own role, so they ... are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college.”

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- Online bullying.

Teaching and support staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood, and signed the staff acceptable use agreement
- They immediately report any suspected misuse or problem to a member of the Designated Safeguard Team for investigation/action, in line with the school safeguarding procedures
- All digital communications with learners and parents/carers should be on a professional level
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or video conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Learners

- Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- Should know what to do if they or someone they know feels vulnerable when using online technology
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website, which contains a copy of the learners' acceptable use agreement
- Publish information about appropriate use of social media relating to posts concerning the school
- Seeking their permissions concerning digital images, cloud services etc (see parent/carer Acceptable Use Agreement in the appendix)
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- Reinforcing the online safety messages provided to learners in school

What are the risks?

Risks to online safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. All staff are the first line of defence; their observation of behaviour is essential in detecting danger to children and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

Potential risks include receiving inappropriate content; predation and grooming; requests for personal information; bullying and threats; identity theft; publishing inappropriate content; online gambling; misuse of computer systems; publishing personal information; hacking and security breaches; corruption or misuse of data.

To ensure that children and staff are adhering to the policy, any incidents of possible misuse will need to be investigated. The school will include online safety in the curriculum and ensure that every child has been educated about safe and responsible use. Children need to know how to control and minimise online risks and how to report a problem.

The online safety policy will be made available to all staff, governors, parents, and visitors through the website. The school will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies.

Teaching and learning – Online Safety Education Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Following Project Evolve (a planned online safety curriculum) in all year groups, which matches to Education for a Connected Work and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

Online Safety Audit

The DfE recommends schools complete the 360-degree safe audit tool. This has been completed by the computing lead and is reviewed termly (with a minimum of termly). Any issues or areas of strength are fed back to SLT and a collaborative approach to action planning is undertaken.

Managing Information Systems

It is important to review the security of the whole system from user to internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly by One IT
- Personal data sent over the Internet or taken off site will be encrypted.
- Staff will use an encrypted memory stick to store all school related data.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The use of user logins and passwords to access the school network will be enforced.

Published content and the school website

- The contact details on the website will be the school address, e-mail and telephone number. Governors, staff or pupils' personal information will not be published.
- The deputy head-teacher will take overall editorial responsibility and ensure that content 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.
- Teaching staff and SLT have log in details for the website. SLT and the SBM have admin rights.

- Teachers are responsible for updating their class page only; any images that are used are to be double checked with a team member; checking the list provided by the office and staff members checking any pupils that are in photographs.

Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the Website or social media, particularly in association with photographs or video.
- Permission from parents or carers will be obtained before photographs or video of pupils are published. Those children who cannot have their photo taken are on a list that is shared with all staff and is displayed in all classrooms.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

Social Media

St John the Baptist Primary School recognises the numerous benefits and opportunities which a social media presence offers. This section aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

- SLT will provide guidance on Social Media use
- SLT will take a lead role in investigating any reported incidents
- The school will control access to social media and social networking sites.
- Staff will monitor, update and manage content posted on school accounts.
- Pupils will use only regulated educational chat environments. This use will be supervised, and the importance of chat room safety emphasised.
- Pupils will be advised never to give out personal details of any kind, which may identify them or their location.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy and the Staff Behaviour Policy.
- The school's Facebook page will be pro-actively monitored by members of staff and inappropriate comments will be removed.

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Managing filtering

- The school's broadband access will include filtering appropriate to the age and maturity of pupils
- Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy
- The school will work with the LA and the internet service provider to ensure that filtering policy is continually reviewed and updated to changes in technology and patterns of online safety
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the Computing lead or Designated Safeguarding lead, who will then record the incident to One IT

Monitoring

The school has monitoring systems in place to protect the school, systems, and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

Mobile Technologies

Mobile technology/devices may be a school owned or privately owned smartphone, tablet, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to our school network, filtering of personal devices, breakages and insurance, access to devices for all learners, network connection speeds, types of devices, charging facilities, total cost of ownership.

Therefore, the school's Acceptable Use Agreements for staff, learners and parents/carers will give consideration to the use of mobile technologies.

Mobile phones and personal devices

- Pupils are not permitted to bring mobile phones or other electronic personal devices, including smart watches, into school. If they do, they will be stored in the school office.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile phones and devices belonging to staff will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be accessed during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose
- Personal devices are brought into school entirely at the risk of the owner and the liability for any loss or damage resulting from the use of the device in school lies with the user (and their parents/carers).

Protecting personal data

- Personal data and sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Schools are audited regularly regarding how they handle their data, for further information please refer to school Information Management Policy.

Communications Policy

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

- The Office 365 school email service is safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school.
- Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Introducing the Policy

- Children will be informed that network and Internet use will be monitored
- Online safety training will be introduced to all to raise the awareness and importance of safe and responsible internet use
- Instruction in responsible and safe use should precede Internet access
- An online safety module will be included in the PSHE, Citizenship or Computing programmes covering both school and home use
- All staff will be given the school online safety policy and its application and importance explained
- Staff should be aware that internet traffic can be monitored and traced to the individual user
- Staff will be made aware that their online conduct out of school could have an impact on their role and reputation 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
- Discretion and professional conduct is essential
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- Parents' attention will be drawn to the school's Online Safety Policy in newsletters, the school website/Marvellous Me, Facebook and on the school learning platform.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents and pupils will be asked to read a form stating that they have read and understood the Acceptable Use document.
- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved on-line materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Stockton LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse will be referred to the head teacher.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure and will need to work in partnership with staff to resolve issues.
- There are clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's online safety ethos.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to online safety.
- The school will ensure appropriate levels of supervision for students/guests who use the internet and technology whilst on the school site.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
 - there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
 - parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
 - online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
 - the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.
-

Appendices

1. Acceptable Use Agreement
2. Acceptable Use Agreement – Staff and Volunteer
3. Acceptable Use Agreement – Pupil KS2
4. Acceptable Use Agreement – Pupil KS1
5. Acceptable Use Agreement – Parent/Carer
6. Rules for Responsible Internet Use
7. Photo Consent Form
8. Useful links

St. John the Baptist Primary School

Acceptable Use

The school has defined what it regards as acceptable/unacceptable use, and this is shown in the appendices below.

Acceptable Use Agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school/ The acceptable use agreements will be communicated/re-enforced through:

- Staff induction and handbook
- School website
- Communication with parents/carers
- Built into education sessions
- Peer support

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

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- Users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Staff (and Volunteer) 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 acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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 policies and the Law.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software & are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

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 ICT Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by: Print Name:

St John the Baptist Primary School Pupil Acceptable Use Agreement – KS2

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of “stranger danger” when I am online
- I will not share personal information about myself or others when online
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else’s work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will not bring my own personal device into school. If I do bring my personal device to school, I will give it to a teacher and know it will be returned at the end of the day.
- Where work is protected by copyright, I will not try to download copies (including music and videos).

- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, parents/carers contacted and in the event of illegal activities involvement of the police.

Pupil Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood, and agree to the rules included in the acceptable use agreement.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: Group/Class:.....
 Signed: Date:

Pupil Acceptable Use Agreement – for KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child):

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

- I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or 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 understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

St. John the Baptist Primary School

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- **I will ask permission before using the Internet.**
- **I will not access other people's files.**
- **I will not use my own software on the school network.**
- **I will only e-mail people my teacher has approved.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **The messages I send will be polite and sensible.**
- **I will not give my name, home address or phone number; or arrange to meet someone, unless this is part of an approved school project.**
- **I will not send photos or video of myself and other pupils unless this is part of an approved school project.**
- **To help protect other pupils and myself, I will tell a member of staff if I see anything I am unhappy with or I receive a message I do not like.**
- **I understand that the school can check my computer files and the Internet sites I visit.**

Consent Form**For Photography and Images of Children**

Dear Parent or Carer

During your child's life at the establishment, we may wish to take photographs of activities that involve your child. The photographs may be used for displays, publications, the school Facebook page and on a website by us, by the Education Authority or by local newspapers. The use of digital images also plays an important part in learning activities. Learners and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Photography or filming will only take place with the permission of the Head Teacher and under appropriate supervision. When filming or photography is carried out by the news, media, children will only be named if there is a particular reason to do so (e.g. they have won a prize), and home addresses will never be given out. Images that might cause embarrassment or distress will not be used nor will images be associated with material on issues that are sensitive.

Before taking any photographs of your child, we need your permission. Please **answer questions below, sign and date the form and return it to the school office.**

Name of Child:		
I understand that:		
• Images may be used to support learning activities • The local media may take images of activities that show the establishment and children in a positive light e.g. Reception Year pictures of new starters, drama and musical performances, sports and prize giving. • Photographers acting on behalf of the school may take images for use in displays, in publications or on a website. • The image will be used in context. • Embarrassing or distressing images will not be used. • The images will not be associated with distressing or sensitive issues, and • The establishment will regularly review and delete unwanted material		
Having read the above statement, do you give your consent for photographs and other images to be taken and used? (Please tick the appropriate box)	☐	Yes , I give my consent for pictures to be taken and used
	☐	No , I do not give permission for pictures to be taken and used
Signature of person responsible for the child:		
Relationship to the child:		
Date (Date/Month/Year)		

NB There may be other circumstances, falling outside the normal day to day activities of the school, in which pictures of children are requested. The establishment recognises that in such circumstances specific consent from parent or guardian will be required before photography or filming of children can be permitted.

Links

UK Safer Internet Centre: saferinternet.org.uk

Childnet: www.childnet.com

Report Harmful Content: This is a reporting website for anyone who has experienced or witnessed harm online. Reportharmfulcontent.com

Common Sense Media, Independent review website for games, apps, TV and movies.
www.commonsensemedia.org

Southwest Grid for Learning, Everything related to online safety. swgfl.org.uk

Internet Matters, Supports families with any online issues. www.internetmatters.org

Swiggle, Child-friendly web browser: swiggle.org.uk

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

e–Safety Officer, Children’s Safeguards Team, Families and Social Care, Kent County Council. The e-Safety Officer is Rebecca Avery email: esafetyofficer@kent.gov.uk Tel: 01622 221469

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children’s Officer for Training & Development, Children’s Safeguards Team, Families and Social Care, Kent County Council. The Children’s Officer for Training & Development is Mike O’Connell email: mike.oconnell@kent.gov.uk Tel: 01622 696677

Children’s Safeguards Team: www.kenttrustweb.org.uk?safeguards

Click Clever Click Safe Campaign: <http://clickcleverclicksafe.direct.gov.uk>

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kidsmart: www.kidsmart.org.uk

Schools Broadband Service Desk - Help with filtering and network security: www.eiskent.co.uk

Schools e–Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: <http://en.teachtoday.eu>

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com