ST BOTOLPH'S CHURCH OF ENGLAND PRIMARY SCHOOL

E-Safety Policy

Review Body:	FGB
Leadership Group Responsibility:	Head Teacher
Type of Policy:	Statutory
Review Period:	Annually
Adopted:	December 2020
Next Review:	September 2021

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

St Botolph's C of E School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles. St Botolph's C of E School has a duty to provide the school community with quality internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the school's management functions. St Botolph's C of E School also identifies that with this there is a clear duty to ensure that children are protected from potential harm online and that procedures are in place with regards to information and recommendations mentioned in Keeping Children Safe in Education (2018) guidance. The purpose of our online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that the school is a safe and secure environment.
- Safeguard and protect all members of our school community online.
- Raise awareness with all members of our school community regarding the potential risks as well as benefits of technology.
- 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 staff including the governing body, teachers, support 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 individuals have been provided with school issued devices for use off-site, such as a work laptops or cameras. 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 Policies, confidentiality and relevant curriculum guidelines including Computing and Personal Social Health and Education (PSHE).

1.2 Links with other policies and practices:

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policies (AUP)
- Behaviour policy
- Child protection policy
- Confidentiality policy

- Curriculum lessons, such as: Computing, Personal Social and Health Education (PSHE)
- Data security
- Image use policy

1.3 Writing and reviewing the online safety policy

St Botolph's C of E online safety policy has been written by the school, involving staff, pupils and parents/carers, building on the KCC online safety policy template with specialist advice and input as required.

The policy has been approved and agreed by the Leadership Team and governing body. The School has appointed the Ethos and Welfare committee from the Governing Board to take lead responsibility for online safety (e-Safety). The school has appointed members of the leadership team as Designated Safeguarding Leads. The school's online safety (e–Safety) Policy and its implementation will be reviewed at least annually or sooner if required.

The School Online safety (e-Safety) Coordinator is Conor Govey

The School Designated Safeguarding Leads (DSL) are Amy Chitty, Janet Harding and Conor Govey

The School Online safety (e-Safety) lead for the Governing Body is The Welfare and Ethos Committee

1.4 Key responsibilities of the community

The school leadership team are responsible for:

- 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.
- Supporting the online safety (e-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 of 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 (pink forms) and using them to inform and shape future practice.
- To work with and support technical staff in monitoring the safety and security of schools systems and networks.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

The safeguarding/online safety leads are responsible for:

- 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 school/setting lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor the school/settings 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.
- Meet regularly with the governor/board/committee member with a lead responsibility for online safety

The staff are responsible for:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of 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 wherever possible.
- Identifying individuals of concern and taking appropriate action by working with the designated safeguarding lead.
- 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 on and off site.
- Taking personal responsibility for professional development in this area.

The staff in charge of managing the technical environment are responsible for:

- Providing a safe and secure technical infrastructure which support safe online 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 and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools 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.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on a safeguarding form, 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.
- Report any breaches on technical infrastructure issues.
- Providing 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/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

The children are responsible for:

- Contributing to the development of online safety policies.
- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.

Parents and carers are responsible for:

- Reading the school/setting Acceptable Use Policies, 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 approaches, 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 encounters online problems or concerns.
- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as Seesaw, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

Managing the school website:

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial 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 administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety on the school website

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 or carers will always be obtained before images/videos of pupils are electronically published.

Appropriate and 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 search the Internet for content.
- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- 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 use is essential.
- Supervision of pupils will be appropriate to their age and ability.
- Pupils will be appropriately supervised when using technology, according to their ability and understanding.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- 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 age-appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- 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.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

Remote Learning:

- St Botolph's C of E Primary will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with pupils and parents/carers will take place using the schools approved communication channels, for example, Seesaw and Google Classroom.
- Staff and pupils will engage with remote teaching and learning in line with existing behaviour principles as set out in our school behaviour policy, staff code of conduct and Acceptable Use Policies.
- Staff and learners will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- When delivering remote learning, staff will:
    - Only use agreed platforms, Seesaw and Google Classroom, to contact learners.
    - Supply work to learners to ensure the school timetable is replicated to the best of their ability.
    - Not record any meetings/sessions on their own devices.
    - Model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

3. Social Media

General use of social media:

- Expectations regarding safe and responsible use of social media will apply to all members of our school community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of St Botolph's C of E School will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of our school.
- All members of our school community are advised not to publish specific and detailed private thoughts, concerns, pictures or personal information of other children at the school 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.
- Inappropriate or excessive use of social media during school hours may result in disciplinary or legal action.

- Any concerns regarding the online conduct of any member of the school 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, whistleblowing, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken, and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, whistleblowing, behaviour and safeguarding/child protection.

Seesaw (school social media platform for communication with parents and pupils):

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be formally approved by the Head Teacher.
- Staff will use school provided email addresses to register for and manage official school approved social media channels.
- All communication on official school social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official school social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by the school will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on Seesaw or official school social media sites/channels in accordance with the school image use policy.
- Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.
- Parents/Carers and pupils will be informed of any official school social media use, along with expectations for safe use and school action taken to safeguard the community.
- Public communications on behalf of the school will, where possible, be read and agreed by at least one other colleague.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff use of social media:

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and that they are an ambassador for the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the school online safety (e-Safety) lead and/or the Head Teacher of any concerns such as criticism or inappropriate content posted online.
- Staff using social media officially will sign the school social media Acceptable Use Policy before official social media use will take place.
- 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 members of 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 media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with line manager/ member of Leadership Team/Head Teacher.
- 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 Head Teacher.
- Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.
- 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 their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with schools policies and the wider professional and legal framework.

- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.
- Members of staff are encouraged not to identify themselves as employees of St Botolph's C of E 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.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.

Pupils' use of social media:

- Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the school Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- 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 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.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

4. Personal Devices and Mobile Phones

Pupils' use of personal devices and mobile phones:

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- Pupils will not be encouraged to bring mobile phones to school; however, we recognise that some of our Year 6 children walk home by themselves or require a phone to make contact with parents/carers. If pupils need a phone for safety reasons, they will be permitted.
- Mobile phones and personal devices will be switched off and handed in to the school office where it will be kept until the end of the day

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 in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with The Head Teacher.
- 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 kept in their lockers in the staff room during the school day.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones / cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices				X				X
Use of personal email addresses in school / academy, or on school / academy network		X						X
Use of school email for personal emails	X							X
Use of messaging apps				X				X
Use of social media		X				X		
Use of blogs		X				X		

Visitors' use of personal devices and mobile phones:

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

5. Policy Decisions

Reducing online risks:

- St Botolph's C of E School 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 educational 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. Schools should include appropriate details about the systems in place.
- The school will take all reasonable precautions to ensure that users access only 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 (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school's leadership team.
- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the school's leadership team

6. Engagement Approaches

Engagement and education of pupils

- An online safety (e-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 Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored using Impero.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Online safety (e-Safety) will be included in the PSHE and Computing programmes of study covering both safe school and home use.
- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.

- The pupil Acceptable Use expectations and Posters 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 and support the school's internal online safety (e-Safety) education approaches
- E-cadets will be recruited and used to support the embedding of E-safety into the school's curriculum and enhance pupil involvement.

Engagement and education of staff

- The online safety (e-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 school safeguarding practice.
- To protect all staff and pupils, the school will implement Acceptable Use Policies which highlights 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 are 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.
- Members of staff with a responsibility for managing filtering systems or to monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school.

Engagement and education of parents / carers

- St Botolph's C of E School recognise 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 (e-Safety) policy and expectations in newsletters, letters, the school prospectus 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 and suggestions for safe home Internet use or highlighting online safety during the year through parent workshops.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on 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. Managing Information Systems

Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Full information regarding the school's approach to data protection and information governance can be found in the schools information security policy

Security and management systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be 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.
- 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 computing coordinator/network manager/IT technicians will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

- All users will be informed not to share passwords or information with others and not to login as another user at any time.

- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.

- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.

- All KS2 pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.

- We require staff and pupils to use STRONG passwords for access into our system.

Filtering Decisions

- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- The school uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and the ICT helpdesk and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately

8. Responding to Online Concerns

- All members of the school/setting community will be aware of online safety incident logs (pink forms) that help to report incidents (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded using the school's safeguarding forms.
- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent 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 and procedure
- Any complaint about staff misuse will be referred to the Head Teacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer) by the Head Teacher.
- Pupils, parents and staff will be informed of the school's 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 cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns 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 the Education Safeguards Team or Kent Police if there is immediate danger or risk of harm.
- 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 Kent Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- Parents and children will need to work in partnership with the school to resolve issues.

9. Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.

- St Botolph's recognises that sexual violence and sexual harassment between children can take place online. Examples may include non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- Our school recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- St Botolph's also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online. We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and Computing curriculum.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learner's electronic devices, they will be managed in accordance with the DfE advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

- Our school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by a DSL.
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- St Botolph's C of E will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented.

- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
  - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
  - Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
  - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
  - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
  - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
  - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Youth Produced Sexual Imagery ("Sexting")

- St Botolph's C of E will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.

- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.
- If learners at other setting are believed to have been targeted, the DSL will seek support from the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at St Botolph's C of E Primary School.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL) will obtain advice through the Education Safeguarding Team.

Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site with filtering systems highlighted previously in this document.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.