St Botolph's Church of England Primary School

Online Safety Policy

September 2022

Introduction

The Online safety Policy relates to all members of St. Botolph's community (including staff, governors, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely. It also relates to other policies including those for Computing, bullying and for Safeguarding and Child Protection.

1.Roles and responsibilities

- The head teacher (Debbie Wilson) has a duty of care to ensure the safety (including online safety) of the whole school community in relation to her role with child protection. The head teacher is also responsible for ensuring all relevant staff receives suitable training. The headteacher will understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident. The Online Safety Lead and technician will support this role with regular monitoring and updating of firewalls, filtering and virus protection. The headteacher will work alongside the OSL to ensure a record is kept of all staff and pupils who are granted access to school ICT systems.

- The Online Safety Lead (Claire Atkinson) will ensure there is regular review and open communication between the Designated Safeguarding Lead (DSL) and themselves. The Online Safety Lead (OSL) will ensure there is an effective approach to online safety to protect and educate the whole school – identifying, intervening and escalating any incident where appropriate and ensure all staff are aware of these procedures. The OSL will take a day to day responsibility for online safety issues and will liaise with the school technician. They will receive reports of online safety issues and create a log of incidents to share with the DSL and school technician. The OSL will work alongside the head teacher to ensure a record is kept of all staff and pupils who are granted access to school ICT systems in 'Record of ICT entitlement'.

- The Governors are responsible for the approval of the Online safety policy and for reviewing the effectiveness of it. The governors will ensure that children are taught about online safety. They will receive information about online safety incidents.

- All staff will understand that online safety is a core part of safeguarding and know who the DSL and OSL are. They must read and follow the Online safety policy and record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures. Staff will oversee the use of technology, encourage sensible use, monitor what pupils are doing and consider potential dangers. All staff will have read, understood and signed the staff acceptable use Policy. They will also ensure that pupils understand and follow the acceptable use policy.

- The Computing Lead (Claire Atkinson) will follow responsibilities listed in the all staff section, plus oversee the delivery of the online safety element of the Computing curriculum. They will work closely with all staff to ensure an understanding of the issues within computing. The computing lead will collaborate with technical staff to ensure a consistent approach.

- The technician (Ark ICT Solutions) will keep up to date with the school online safety policy in order to effectively carry out their online safety role. They will ensure the

technical infrastructure is secure and is not open to misuse or malicious attack. The technician will ensure that staff may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. The technician will work closely with the DSL and OSL to ensure the school systems reflect the school policy, supporting and advising where necessary. They will regularly monitor and update firewalls, filtering and virus protection. The technician will report any online safety related issues, in line with the school policy.

- Volunteers and school visitors will read, understand, sign and adhere to an acceptable use policy. Report any concerns, no matter how small, to the designated safety lead / online safety lead as named in the AUP. Volunteers will model safe, responsible and professional behaviours in their own use of technology.

- Pupils will read, understand, sign and adhere to the pupil acceptable use policy and review this annually. They will understand the importance of reporting abuse, misuse or access to inappropriate materials and do so to an adult. Pupils will know what action to take if they or someone they know feels worried when using online technology. Pupils will understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media if it relates to school. Pupils will understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

- Parents will be told how to access a copy of the pupil's acceptable use policy (AUP) and will be encouraged to support their children in following it. Parents will be encouraged to consult with the school if they have any concerns about their children's and others' use of technology. Parents and carers attention will be drawn to the school online safety policy in newsletters, the school brochure and on the school website. They will promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

- Our Online safety Policy has been developed by the school, building on the government guidance and advice from Lincolnshire Safeguarding Board, London Grid for Learning and South West Grid for Learning. It has been agreed by senior management and approved by governors.

2. Education and Curriculum

The school will be using materials from 'Project Evolve' for our Digital Literacy lessons. Project Evolve is based on UKCIS framework 'Education for a connected world', covering knowledge, skills, behaviours and attitudes across eight strands of our online life. Each class will have one stand-alone Digital Literacy lesson per term. This has been mapped to coincide with the computing curriculum and the strands which are covered through it, in each year group. The class teacher will select the most appropriate objective for their class, depending on each classes' individual needs.

2.1 Pupils

- The school will ensure that the use of Internet derived materials by pupils acknowledges the source of information and complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be helped to understand the need for the Pupil Acceptable Use Policy, and encouraged to adopt safe and responsible use both within and outside school
- Pupils will have good role models
- Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.
- A digital literacy/online safety curriculum should be provided as part of computing/PSHE/other lessons and should be revised regularly
- Key online safety messages should be reinforced through planned assemblies and classroom activities.
- When pupils can freely search the internet staff should monitor websites visited.

2.2. Parents

Many parents and guardians have limited understanding about the risks and issues of online safety. The school will endeavour to provide information and awareness to parents and guardians through:

- Curriculum activities
- Letters, newsletters and the school website/social media
- Parents evenings
- Awareness Days e.g. Safer Internet Day
- Direction to suitable websites.

2.3 Staff

- A digital literacy/online safety curriculum should be provided as part of computing/PSHE/other lessons and should be revised regularly.
- Staff will be required to read and fully understand the online safety policy and the Acceptable Use Policy.
- Staff will be required to complete online safety training annually.
- Staff can receive guidance from the OSL and DSL when required.
- The school will ensure that the use of Internet derived materials by staff complies with copyright law.

3 Filtering, monitoring and infrastructure

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Lincolnshire County Council can accept liability for any material accessed, or any consequences of Internet access.

- The school will work with the Ark ICT Solutions, LSB and LCC to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to an adult in school who will report this to the OSL.
- All Foundation and KS1 pupils will use a class log in when using laptops and computers.
- All KS2 pupils will use an individual log in when using laptops and computers.
- All other required usernames and passwords – TTRS, Scratch etc. will be administered by the Ark technician or the Computing lead.
- The internet is filtered for all users in school. Requests for changes need to be thoroughly checked and sent to the Ark technician.
- A procedure is in place (see pupil AUP) for pupils to report any concerns regarding technical or security issues.
- Security measures are in place to protect the school system.

4 Use of digital and video images (including publishing)

- Whenever a photo or video is taken it will only ever be stored on the device it was taken, the school network or the school cloud storage.
- When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose.
- Whenever a photo or video is taken/made, the member of staff will check the database before using it for any purpose.
- Any pupils shown in public materials are never identified with more than their first name.
- Staff and parents are reminded regularly about the importance of not sharing without permission.
- Members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and always moved to school storage as soon as possible and deleted from personal devices.
- Care should be taken when taking digital images/videos that pupils are appropriately dressed and are not taking part in activities that may bring the individuals or the school into disrepute.
- Video conferencing and the use of webcams should use the educational broadband network to ensure quality of service and security, if needed.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised by school staff.
- All staff will encourage pupils to think about their online reputation and digital footprint.
- Pupils will be taught about how images can be manipulated in their digital literacy curriculum.
- Pupils will be taught that they should not post images or videos of others without their permission.

5 Data protection and data security

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.
- When personal data is stored on any portable computer system, memory stick or any other removable media, the device must be password protected and the data securely deleted from the device once it's use is complete.

6 Communications

6.1 E-mail and other communication

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will carefully monitor how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, Virtual Learning Environment etc) must be professional in tone and content.
- All parents and staff will be invited to provide a mobile telephone number(s) to receive electronic communication via ParentMail.
- Only authorised staff (Head, Deputy, Senior Administrator and Administrative Assistant) will have access to ParentMail.
- Parents' details will be deleted from ParentMail on request, or when their child(ren) leaves the school.
- ParentMail will also be used to communicate with staff and governors and relevant outside bodies as appropriate. E.g. in the event of an emergency closure.

6.2 Introducing the Online safety policy to pupils

- Annually pupils will read, discuss and sign the Pupil AUP.
- Online safety rules will be discussed with pupils regularly.
- The Online safety Policy will be posted on the school website for parental benefit.
- Pupils (where appropriate) will be informed that network and Internet use will be monitored and appropriately followed up.

7 Social Media and website (including publishing of images and work)

7. 1 Social networking

- The school manages and monitors our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.
- Any messages published on the school social networks should protect the pupils, the school and the staff.
- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Social networking sites such as Facebook; Twitter; Instagram and Snapchat are permanently blocked by ICT provider. Pupils cannot log onto or search these sites in the school environment.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised of the risks and told to strongly consider the use of nicknames and avatars if using social networking sites outside of school.
- The school will make every effort to support parents at home, signposting relevant materials e.g. CEOPs so that pupils and parents are fully aware of online risks.
- We will ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.
- Staff will also not encourage or condone underage use, but will acknowledge reality in order to best help our pupils avoid or cope with issues, should they arise.
- Parents, staff and pupils are expected to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face. This applies to both public pages and to private posts, pages or groups.

7.2 Personal publishing

- Parents must request permission to record e.g. video pupils at school and the school will keep a record of all such requests. Parents must only take photographs for personal use.
- Parents must not publish images/photographs/video of pupils (other than their own) or staff, or personal information about school-based events on social media sites. Any reported breaches will be subject to scrutiny and explored by the school.

7.3 Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

7.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that their image cannot be misused. Pupils' photographs will only be used if parental consent has been given.
- Pupils' full names will not be used anywhere on the school website in association with photographs.
- Written permission from parents or carers will be obtained when children join the school. Photographs of pupils will not be published on the school website without permission.
- Work can only be published with the permission of the pupil and parent/carers.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

8 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.
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones are not permitted in school. Any necessary phone calls will be made by school staff. Pupils to hand in mobile phones to class teacher until home time as they walk home independently.
- Nintendo DSi's, iPods, iPads and other personal games consoles systems which may have non-filtered internet connections will not be permitted in school.
- Staff will be issued with a school camera (iPad) to capture photographs of pupils.

9 Handling online safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding. General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Any complaint of pupil misuse, either at home or at school, must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and then reported to the OSL to take appropriate action
- We will inform parents/carers of online-safety incidents involving their children. More serious behaviour which staff or pupils may be engaged in or subject to, may involve the CEOP or/and police.

9.1 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.