Viam Parabimus

St. John the Baptist
Catholic Primary School

We will prepare the way by loving, living and learning with the Lord

Online Safety Policy

Audience: Staff/ Governors/ Public
Frequency of Review: Annually
Postholder Responsible for Review: Computing Leader

Recommended Associated Documents:
Child Protection Policy
GDPR Data Protection Policy
Computing Policy
Anti-Bullying Policy
Digital Images Policy
Acceptable Use Policy
Mobile and Wearable Device Policy
PSHE Policy

Approved by the Full Governing Body – March 2021
Review – March 2022

Writing and reviewing the Online Safety Policy

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, anti-bullying, digital images, Mobile and wearable devices, PSHE, Child protection and the GDPR Data protection policy.
The school has an appointed Online Safety Coordinator: Sarah Day who will have responsibilities delegated from Ian Gallagher (Headteacher & DSL) and Helen Dixon (Deputy Head & DSL).
Our Online Safety Policy has been written by the school, building on the Solihull Online Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

Online Safety Group

The school has an Online Safety Group that consists of Designated Safeguarding Lead (Ian Gallagher), Online Safety Coordinator (Sarah Day), Child and Family Support Worker (Sarah Clarke) and our pupil voice the KS2 eCadets.
The group will meet termly to discuss any online safety concerns, review Online Policies, look at current or new online safety risks to our school and discuss what we are doing in school to ensure our staff and pupils stay safe online.

eCadets

eCadets is a structured pupil-led peer empowerment Online Safety program that is being implemented in KS2 in our school. The eCadets learn about Online Safety and use their knowledge and skills to carry out tasks/challenges as a group and with their peers to ensure that all children in our school stay safe online.

Policy Decisions

Authorising Internet access

- All adults working within school must read and sign the Staff Acceptable Use Policy before using any school ICT resource.
- The school maintains a current record of all staff and pupils who are granted access to school ICT systems.
- Pupil access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a child’s AUP consent form.
- Any user accessing the school ICT system will be asked to consent to AUP every time that they log on to the school network.

Assessing risks

- 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 Solihull Local Authority accepts liability for any material accessed, or any consequences of Internet access.
- The school audits ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

Handling online safety complaints/incidents

- Online Safety incidents or complaints will be recorded on the concerns form (Appendix 1) and handed to either the Online Safety coordinator or the DSL and the procedures followed in accordance with the Online Safety incident report procedures (See Appendix 2)
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (see Child Protection Policy).
- Pupils and parents are informed of the complaints procedure (see school's Complaints Policy)
- Pupils and parents are informed of consequences for pupils misusing the Internet.

Use of the Internet beyond the school day

- The school liaises with community organisations (before/after school care) and parents/carers to establish a common approach to online safety.
- When using Social Media sites (Facebook, Instagram, Snapchat, Twitter, Tiktok etc..) for a personal nature, staff are aware that they ensure that the maximum privacy settings are used and that they will not be used to discuss the school, parents or pupils (see Acceptable Use Agreement and Social Media Policy).

Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. *We have a managed system so that it gives children a greater understanding of how to stay safe as they can assess and manage some risks themselves.*
- The school Internet access is monitored using software (Future Digital) that will take screen snapshots of any suspicious use. This will allow the children to access the internet with reduced filtering.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet, in order to locate, retrieve and evaluate information.
- Pupils are shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content by minimising screen, closing the lid of a laptop or turning a tablet device over.

Communications Policy

Introducing the online safety policy to pupils

- Online safety rules and objectives are posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils are informed that network and Internet use is monitored and appropriately followed up.
- A programme of training in online safety will be undertaken by staff as appropriate.
- Online Safety training is embedded across all areas of the curriculum.

Staff and the Online Safety Policy

- All staff are given the School Online Safety Policy and its importance is explained.
- Staff are informed that network and Internet traffic can be monitored and traced to the individual user using the Future Digital Monitoring software.
- Staff always use a child friendly safe search engine when accessing the web with pupils.
- All new staff should receive Online Safety training as part of their induction programme ensuring they fully understand the schools Online Safety policy and Acceptable Use Agreement.
- Digital communications by staff must be professional and respectful at all times and in accordance with the Social Media policy.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- The school will seek to provide information and awareness to Parents/Carers regarding Online Safety through:
  - Newsletters
  - School website
  - Social Media (Twitter)
  - High profile events (e.g. Safer Internet Day, Anti-Bullying Week)
  - Reference to relevant websites

Managing Internet Access

Information system security

- School ICT systems security is reviewed regularly.
- Virus protection is updated regularly.

- Security strategies are discussed with the Local Authority.
- Solihull Local Authority monitor the school system and any unusual, suspicious or inappropriate use will be reported to Ian Gallagher (Headteacher).

Email

- Staff and pupils may only use Solgrid email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- Pupils will only use school email to email people they know.
- The forwarding of chain letters is not permitted.

Publishing pupil's images and work (See Images Policy)

- Pupils' full names will not be used anywhere on the school website or other online space, particularly in association with photographs.
- Written consent must be gained from parents/carers when using digital images of pupils (see the images policy) on the school website, social media and media
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing filtering

- The school works with Solihull Local Authority 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 the Online Safety Coordinator and DSL and this is then reported to the Local Authority.

Managing video conferencing & webcam use

- Video conferencing uses the educational broadband network to ensure quality of service and security.
- Video conferencing and webcam use will be appropriately supervised for all pupils.

Managing emerging technologies

- Emerging technologies are examined for educational benefit before use in school is allowed.

- Mobile phones and wearable devices will not be used during lessons or formal school time by staff (See the Mobile and Wearable Device Policy). Children should not wear wearable devices to school and only children in Year 6 who need a mobile phone due to walking home alone are permitted to bring a mobile phone to school. They must be given to the school office at the start of the day and collected again at the end of the school day.
- Appropriate use of the digital technology is detailed in the School's Acceptable Use Policy.
- Staff will only use iPads and tablets owned by and registered to the school to take photographs of children.
- Staff should only use iPads for information relating to school use.

Protecting personal data

- Personal data is recorded, processed, transferred and made available according to the GDPR Data Protection Policy.
- Memory sticks and laptops must be encrypted according to Local Authority policy.
- Staff and pupils are aware that they <u>must not</u> give their username and password to any other individual and that passwords will be changed regularly (see the school Acceptable Use Agreement)
- Staff and pupils are aware that they must respect system security and not disclose any password or security information to anyone other than an authorised system manager (see school Acceptable Use Agreement).

<u>Children and Online Safety Away from School</u>

- St John's will ensure any use of online learning tools and systems are in line with privacy and data protection/GDPR requirements.
- All procedures and expectations stated in this Online Safety Policy must continue to be adhered to.
- Parents will be reminded of the support available to them in order to help to keep their children safe online through the school newsletter and links on our school website.

Home Learning

- The majority of home learning will be set using learning platforms provided by the school such as: Class Dojo and Microsoft Teams
- These are secure authenticated platforms for which children have unique logins
- Where children are directed to alternative websites, for example to access video resources, staff will check the suitability of the content before directing children to access them
- Staff will wear suitable clothing, as should anyone else in their household if recording or videoing, e.g. a story time session for children
- Staff will be mindful of what can be seen in the background if making a recording.
- Language must be professional and appropriate at all times, including any family members in the background.

Communication

- Staff must only use platforms provided by the school (such as: Class Dojo and Microsoft Teams) to communicate with pupils
- Children are able to communicate via email with teachers through their school email
- Staff are able to access children’s emails, including deleted ones, if any concerns should
- arise.
- Where possible calls to children will be made from school telephones.
- When this is not feasible and staff are calling children from their own telephones, they will always use 141 before dialling so as not to share their personal telephone numbers

Appendix 1

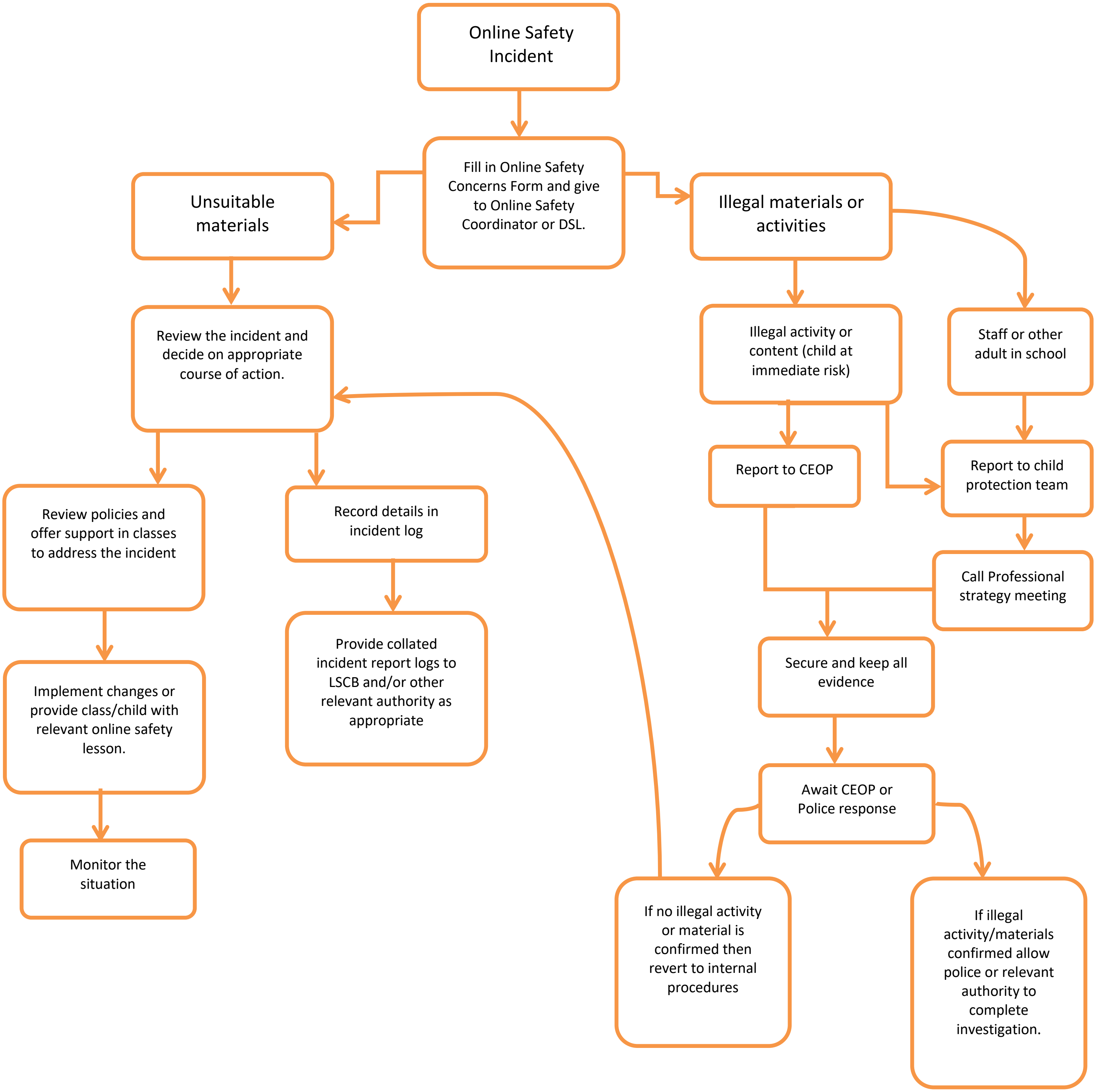
St John the Baptist Catholic Primary School

Online Safety Concerns Form

Name of child/family:	Class:
Date:	Time:
Name of staff member raising concern:	
Concern:	
Name and signature of DSL:	
Action by school:	

Appendix 2

St John the Baptist Online Safety Incident Report Procedures


Online Safety Incident
Fill in Online Safety Concerns Form and give to Online Safety Coordinator or DSL.
Unsuitable materials
Illegal materials or activities
Review the incident and decide on appropriate course of action.
Illegal activity or content (child at immediate risk)
Staff or other adult in school
Report to CEOP
Report to child protection team
Review policies and offer support in classes to address the incident
Record details in incident log
Call Professional strategy meeting
Implement changes or provide class/child with relevant online safety lesson.
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Secure and keep all evidence
Await CEOP or Police response
Monitor the situation
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity/materials confirmed allow police or relevant authority to complete investigation.