# e-Safety Policy

St Mary’s Catholic Primary School

Mission Statement

LEARNING TO LIVE OUT OUR CALLING WITH COMPASSION AND LOVE

# E-Safety Policy

E-Safety encompasses internet technologies and electronic communications such as mobile tablets as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using online technology and provides safeguards and awareness for users to enable them to control their online experience. The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Safeguarding.

**End to End E-Safety**

E-Safety depends on effective practice at a number of levels:

- Annual certified training provided by the National College for Online Safety designed to meet the statutory online safety duties of the Keeping Children Safe in Education document.

- Responsible ICT use by all staff and students encouraged by education and made explicit through published policies.

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband from the Staffordshire Education WAN including the effective management of Smoothwall filtering. Use of SENSO software to monitor and respond to use any inappropriate user use.

- National Education Network standards and specifications.

## School E-safety policy

## Teaching and learning

**Why are new technologies and Internet use important?**

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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.

**How will internet use enhance learning?**

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.

**How will pupils be taught to evaluate Internet content?**

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**How will pupils be taught to stay e-safe?**

- Curriculum planning will include age appropriate opportunities to discuss, role play and learn about the benefits and risks offered by new technologies, such as e-mail, mobile phones and social networking sites.
- E-safety delivery will be mapped across the curriculum to ensure full coverage. E-safety lessons will be taught through explicit units of work in the RSE and Computer Curriculum.
- E-Safety ambassadors will be trained to deliver monthly assemblies to KS2 (potentially KS1 in Summer). They will share updates to E-safety policies and news from NOS webinars.

## Managing Internet Access

## Information system security

- Virus protection will be updated regularly by the ICT Technician on all networked computers.
- School ICT systems capacity and security will be reviewed regularly using the Forensic software tool.

**E-mail**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
    - Do not delete this email before telling a teacher.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission

**Public Web published content and the school web site**

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- E-mail addresses will be published carefully, to avoid spam harvesting.
- The Headteacher, Office staff and Computing Leader will take overall editorial responsibility and ensure that content is accurate and appropriate. Even though all class teachers will be responsible for their own class and subject pages.
- The website should comply with the school's guidelines for publications, including respect for intellectual property rights and copyright.

**Web Publishing pupils' images and work**

- Images, published to the web, that include pupils will only contain pupils who have appropriate, written permissions collected by the class teachers.
- Pupils' full names will not be used anywhere on the website in association with photographs.

**Social networking and personal publishing**

- The Internet provider (Stone Assist) /school will block/filter access to social networking sites i.e. Facebook, Bebo, Myspace, except those specifically purposed to support educationally approved practice.
- Staff and pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces, outside school based controlled systems is inappropriate for primary aged pupils, unless strictly supervised.
- Staff and pupils should be advised not to publish specific and detailed private thoughts on social networking sites.

**Managing filtering**

- The school will work with the Technical Support team (Staffs Tech) and the Internet Service Provider (Stone Assist) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, the URL must be reported to the school filtering manager Mr M. Holmes (CtKCC Lead Technician), the e-Safety Leader in school (Miss Heath ) or the Service Provider helpdesk (Staffs Tech).

- If an unsuitable website is detected, please notify the school E-Safety Leader and ensure that the website is reported.

**Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time, unless specifically allowed to support learning as identified by the teacher. The sending of abusive or inappropriate text messages is forbidden.

**Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) Act 2018

## Policy Decisions

### Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications, which includes internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- All staff must read and sign the 'CTKCC Acceptable Use Policy' (see appendix 1) before using any school ICT resource.
- At Foundation Stage and Key Stage 1 access to the Internet will be by adult demonstration or by directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form (see appendix 2)

**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 the MAC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision annually to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

- Methods to identify, assess and minimise risks will be reviewed by the Technical Support Team.

**Handling e-safety complaints**

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues. Sanctions within the school discipline policy will include:

o Interview with senior staff member;

o informing parents or carers;

o removal or restriction of Internet or computer access for a period.

- Discussions will be held with the local PCSO if possible to establish procedures for handling potentially illegal issues.

***See appendix 3 for 'Response to an incident of concern'***

**Community use of the Internet**

- The school will liaise with local organisations to establish a common approach to esafety.

**Cyberbullying – Understanding and addressing the issues**

While cyberbullying is likely to be low level in primary schools, the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or social media, are becoming more frequent.

As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.

As felt appropriate for the age and use of technology by the pupils:

- The CTKCC Anti-Bullying Policy and the school's Positive Behaviour Policy will address cyberbullying. Cyberbullying will also be addressed in ICT, PSHCE, assemblies and other relevant lessons and is brought to life through activities. As with other whole school policies, all staff and young people will be included and empowered to take part in the process.

- Pupils, parents, staff and governors will all be made aware of the consequences of cyberbullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.
- Parents will be provided with an opportunity to find out more about cyberbullying through: session for parents, guidance, access to the National Online Safety site

**Cyberbullying - How will risks be assessed?**

- The school will take all reasonable precautions to ensure against cyberbullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor CTKCC, can accept liability for inappropriate use, or any consequences resulting outside of school.
- The school will proactively engage with KS2 pupils in preventing cyberbullying by:
    - understanding and talking about cyberbullying, e.g. inappropriate use of email, text messages;
    - keeping existing policies and practices up-to-date with new technologies;
    - ensuring easy and comfortable procedures for reporting;
    - promoting the positive use of technology;
    - evaluating the impact of prevention activities through questionnaires or class discussions

- Records of any incidents of cyberbullying will be logged on My Concern and will be used to help to monitor the effectiveness of the school's prevention activities.

**How will cyberbullying reports/issues be handled?**

Complaints of cyberbullying will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Headteacher.
- Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyberbullying.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
    - interview/counselling by the class teacher;

  - informing parents or carers;
  - removal of Internet/computer access for a period

## Communications Policy

### 2.5.1 Introducing the e-safety policy to pupils

- An E-safety assembly will be conducted by the Computing leader and KS2 E-safety officers to the whole school.
- Pupils will be informed that the school network and Internet use will be monitored. Children are regularly involved in creating posters with rules for around the school.

### Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its application and importance explained.
- All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided by National Online Safety at the start of the academic year.

### Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, on the school website and through the use of the National Online Safety website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This may include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

## Appendix 1: Acceptable use policy for Staff

# *Staff Information Systems Code of Conduct*

**September 2022**

*To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this Code of Conduct. Staff should consult the school's e-safety policy for further information and clarification.*

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role.

- I understand that school information systems may not be used for social media or private purposes, without specific permission from the headteacher.

- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.

- I will ensure that all confidential and assessment data about pupils is securely saved and password protected.

- I will not install any software or hardware without permission.

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.

- I will ensure that any electronic communications with pupils are compatible with my professional role.

- I will not publish any content which might put myself or the school in a compromising situation, breech the school's confidentiality in any way or bring the school's reputation into disrepute.

- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

*The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.*

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …………………………………… PRINT: ………………….……………… Date: …………

Accepted for school: ……………………….……………. PRINT: ………………….……………….

## Appendix 2: Parent and Pupil consent form

**Mary's Catholic Primary School**

# e-Safety Rules

***All pupils use computer facilities, including Internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.***

| | |
|---|---|
| ***Pupil:*** | ***Class:*** |

**Pupil's Agreement**

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access is monitored for inappropriate use.

| | |
|---|---|
| ***Signed:*** | ***Date:*** |

**Parent's Consent for Web Publication of Work and Photographs**

I agree that my son/daughter's work may be electronically published. I also agree that appropriate media that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

**Parent's Consent for Internet Access**

I have read and understood the school e-safety Rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

| | |
|---|---|
| ***Signed:*** | ***Date:*** |

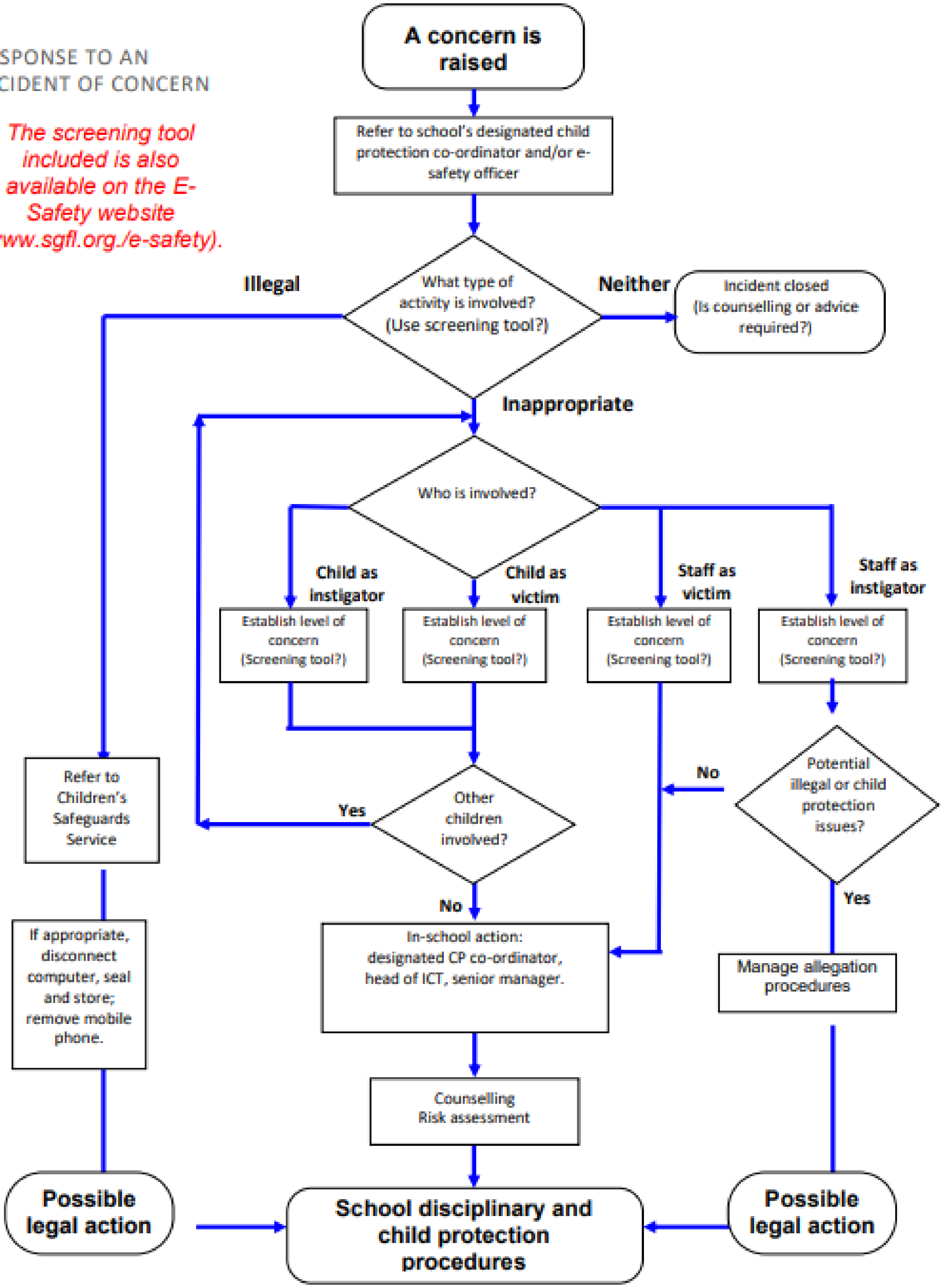
***Please print name:***

**Please complete, sign and return to the school office**

## Appendix 3: Response to an incident of concern

RESPONSE TO AN INCIDENT OF CONCERN

*The screening tool included is also available on the E-Safety website (www.sgfl.org./e-safety).*



A concern is raised
Refer to school's designated child protection co-ordinator and/or e-safety officer
What type of activity is involved? (Use screening tool?)
Illegal
Neither
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern (Screening tool?)
Establish level of concern (Screening tool?)
Establish level of concern (Screening tool?)
Establish level of concern (Screening tool?)
Refer to Children's Safeguards Service
If appropriate, disconnect computer, seal and store; remove mobile phone.
Yes
Other children involved?
No
No
Potential illegal or child protection issues?
Yes
In-school action: designated CP co-ordinator, head of ICT, senior manager.
Manage allegation procedures
Counselling Risk assessment
Possible legal action
School disciplinary and child protection procedures
Possible legal action