St. Winefride’s Catholic Primary School

Online Safety Policy

CONTENTS

1. AIMS AND PURPOSE

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree to implement the school's approach to online safety. The policy relates to other school policies including, but not limited to, the Computing and Technology Policy, Behaviour for Learning Policy, Health & Safety Policy and Safeguarding Policy.

2. TEACHING AND LEARNING

2.1. Why Internet use is important

- The Internet is an essential element of 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 part of the statutory curriculum and a necessary tool for both staff and pupils alike.

2.2 Internet use to enhance learning

- The school Internet access is designed expressly for staff and pupil use and includes London Grid for Learning (LGFL) filtering, appropriate to the level required.
- Pupils will be taught what Internet use is acceptable and what is not, they will be given clear objectives for their Internet use.
- Pupils will be educated in the effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation.

2.3 How pupils will be taught to evaluate Internet content

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

3. MANAGING INTERNET ACCESS

3.1 Computing and Technology system security

- The school's computing and technology systems capacity and security will be reviewed regularly in conjunction with the school based technician (SBT) from Newham Partnership Working (NPW), our computing and technology service providers.
- Virus protection will be updated regularly by our SBT.

3.2 E-mail content and the school website

- Pupils may only use their LGFL designated email address (i.e. not their personal email address) whilst on the school premises. They should not use mobile devices to access any other email or messaging service while at school.
- The contact details on the school's website shall be limited to:
  The school's address
  The school's telephone and fax numbers
  The school's email address.

- Staff and pupils' personal information will not be published on the website under any circumstances.
- The Headteacher, or a responsible person nominated by them, will take overall editorial responsibility for information published on the website and will ensure that content is accurate and appropriate.

3.3 Publishing pupil's images and work

- All parents/carers will be asked to read and sign the document 'Use of digital images - photography and video'.
- Photographs that include pupils will be selected carefully and will not include children whose parents/carers have requested that their children's images are not used.
- If an image of a child is used on the website or on a similar document, such as but not limited to the school prospectus, their name will not be associated with that image. Similarly if a child's name is mentioned then their image will not be used in conjunction with it.
- Pupil's work may be published on the school website but, as above, only an image or the name of the pupils will be used not both.

3.4 Social networking and personal publishing

- The school network is filtered by LGFL and automatically blocks social networking sites, instant messaging sites and many email providers at source. We strongly recommend that parents monitor their children's use of social networking sites and particularly any apps or sites that send instant messages and images. Although the recommended age to join and/or download these apps and services is often if not always higher than primary school age, we recognise that children are still able to do so, therefore it is imperative that parents engage with their children's internet activity at all times.

3.5 Managing filtering

- The school will continually work with LGFL, NPW, the SBT, DfES and all concerned agencies to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Computer and Technology coordinator, the SBT or the Health and Safety Officer.

3.6 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before any new technology is used in school.
- Mobile phones are not to be used by pupils or staff during school/class time. Pupils will be allowed to bring mobile phones to school but they must be handed in to the class teacher at the beginning of the school day. They will be returned when the pupil leaves school for the day. It is the responsibility of the pupil to turn off their mobile phone before it is handed in to their teacher.
- Staff are allowed to use their mobile phones during breaks and non-contact time, although not at the expense of completing their work.

3.7 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the world wide scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never be accessed on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access by any individual.

3.8 Handling online safety complaints

- The Headteacher will deal with complaints of internet misuse.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the school Child Protection and Safeguarding Procedures.

3.9 Community use of the internet

- All use of the school internet by members of the community and other organisations (e.g. if hiring school premises for clubs or functions) must be approved before use and is subject to the same conditions and restrictions as per normal school practice in accordance with the Online Safety Policy, which must be given to any potential user.

3.10 Introducing the online safety policy to pupils

- The children will be asked to read and sign, where appropriate, the '12 Rules for Responsible Computer and Technology Use' and the 'Pupil Online Safety Agreement'.
- Online safety rules will be discussed with the pupils at the start of each year.
- The '12 Rules for Responsible computer and Technology Use' will be displayed in each classroom so that all users may see them.
- Pupils are reminded that all network and internet use is monitored and dealt with appropriately.
- The pupils will receive online safety lessons and are constantly reminded of online safety.

3.11 Staff and the online safety policy

- All staff will have access to this policy and its importance explained.
- Staff will be made aware that internet use may be monitored.
- Discretion and professional conduct is essential.
- Staff will always use a child friendly search engine when accessing the web with pupils.
- Staff will always watch any downloaded videos in their entirety before showing them to the children.
- When showing videos from sites such as, but not exclusively, Youtube, Vimeo etc. staff will ensure that any attached comments are either appropriate or the comments are disabled.

3.12 Enlisting parent's support

- Parent's attention will be drawn to the School Online Safety Policy in newsletters and during events such as the weekly Coffee Morning.

3.13 If using the internet at home

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they should report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Pupils should only invite known friends to conversations etc. and block or deny access to uninvited or unsolicited requests from others.
- Parents should always be in control of their children's internet use at home. Parents should be especially careful of their children's access to the internet via mobile devices. Many games consoles actively encourage children to participate in games connected to the internet and these often feature interaction between players possibly from all over the world. While this is a wonderful way of children communicating with people from different countries and cultures it is also a way for undesirable people to contact children, therefore do not assume that 'it is only a game', and keep a close watch on all internet access.
- Mobile phones and tablets are now as powerful as most laptops and desk top computers. Parents should ensure that their children's phones etc. are suitably safeguarded using the parental controls to prevent unwanted websites etc. being available on these devices. Also parents must be aware of the potential dangers when letting their children use their (the parents) phone. Are these devices secure and safe for children? Could a child inadvertently pay for upgrades etc. while playing a game? Is it possible for children to use a search engine on the phone that does not have parental controls set? Does the child have access to the parent's password; if so is it possible for them to re-set the parental controls or override a blocked access point?

4. ONLINE SAFETY INCIDENT LOG

Number:	**Reported by:**		**Reported to:**
Date Reported:			
Incident description: (Describe what happened, to whom it happened or who was responsible and what action was taken)			
Review Date:			
Result of Review:			
Siganture: Headteacher		**Date:**	
Signature: Governor		**Date:**	

5. RISK LOG

Risk Log (Example risks Shown)

No	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	Online Safety Officer, C and T Coordinator
2	Internet browsing	Access to inappropriate/illegal content - pupils	2	3	6	
3	Pupils internet use at home	Access to inappropriate/illegal content at home	3	3	9	
4						
5						

Likelihood: How likely is it that the risk could happen (foreseeability).

Impact: What would be the impact to the school (e.g. in terms of legality, reputation, complaints from parents, etc.)

Likelihood and impact are rated between 1 and 3, with 1 being the lowest.

Score: 1 -3 = Low Risk

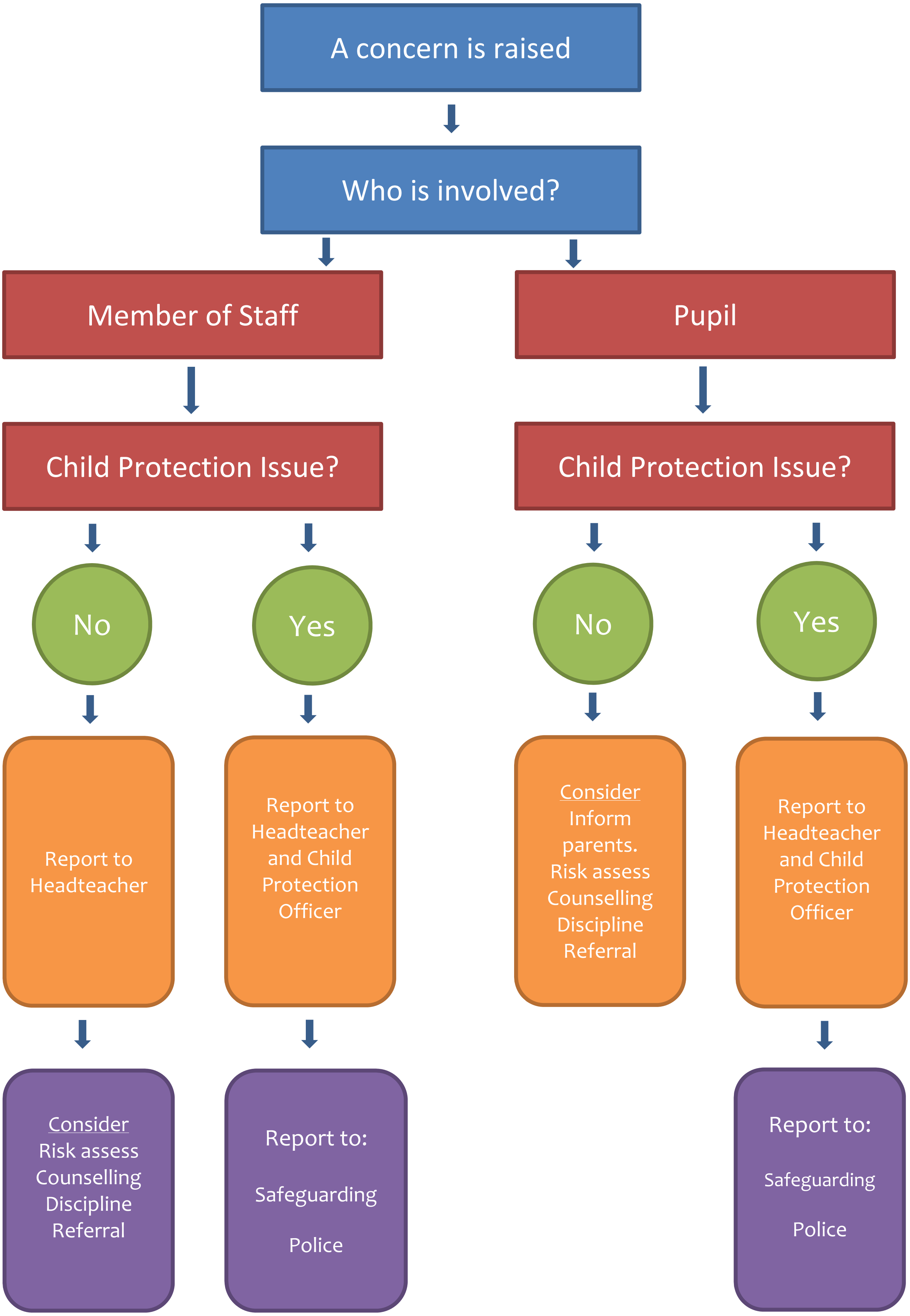
4 -6 = Medium Risk

7 - 9 = High Risk

Owner: The person who will action the risk assessment and recommend the mitigation to the Headteacher and Governing Body.

The Final decision rests with the Headteacher and Governing Body.

6. Inappropriate Activity Flowchart



A concern is raised

Who is involved?

Member of Staff

Child Protection Issue?

No

Report to Headteacher

Consider
Risk assess
Counselling
Discipline
Referral

Yes

Report to Headteacher and Child Protection Officer

Report to:

Safeguarding

Police

Pupil

Child Protection Issue?

No

Consider
Inform parents.
Risk assess
Counselling
Discipline
Referral

Yes

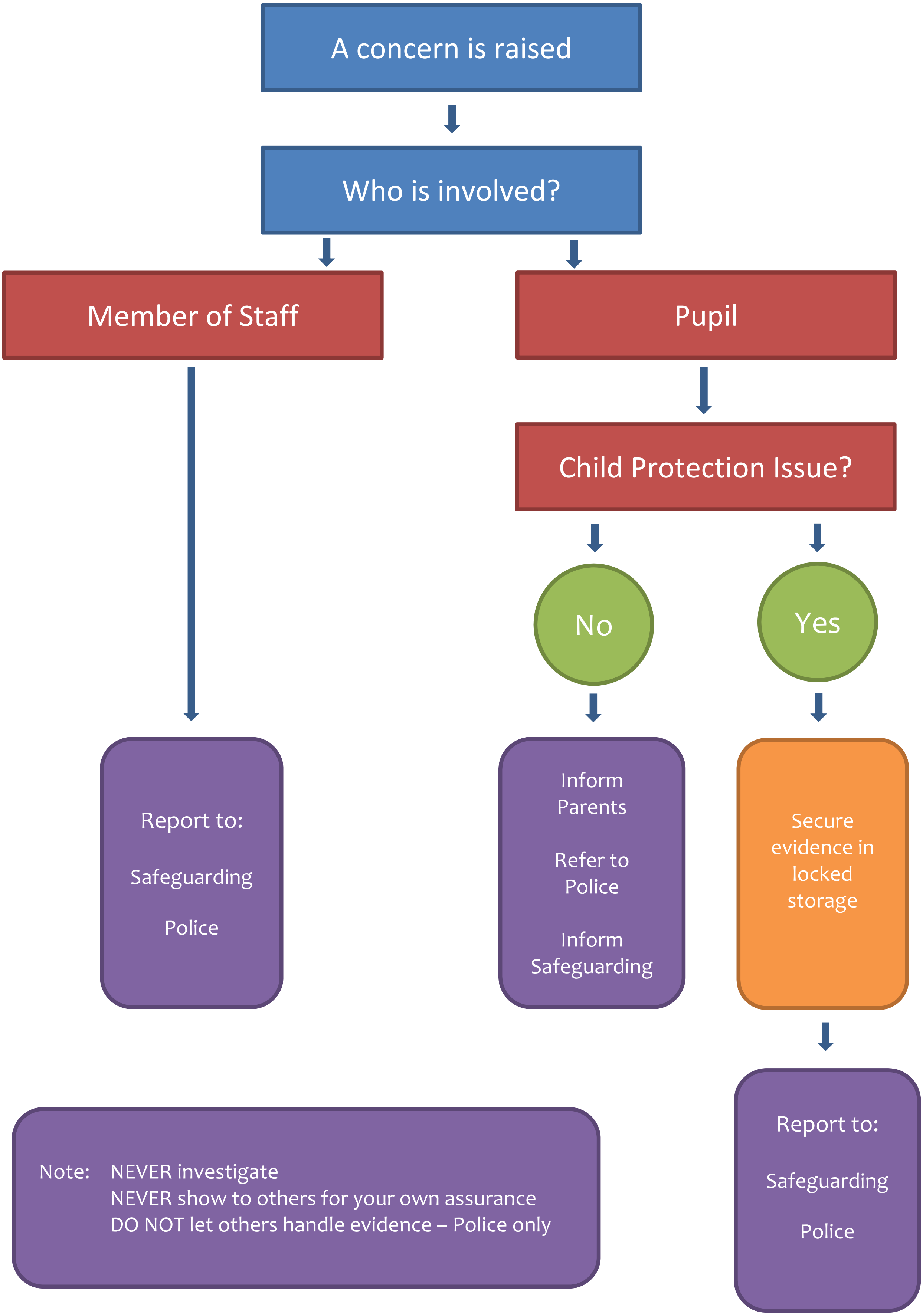
Report to Headteacher and Child Protection Officer

Report to:

Safeguarding

Police

7. Illegal Activity Flowchart



Note: NEVER investigate
NEVER show to others for your own assurance
DO NOT let others handle evidence – Police only

8. MONITORING AND REVIEW

It is the role of a named school governor with responsibility for Computing and Technology to monitor the policy and practice of computing. The governor concerned liaises with the Headteacher and Computing and Technology Coordinator before reporting to the governors on Computing and Technology.

By order of the Governing Body of St Winefride's Catholic Primary School

(Signed) ______________________________________
(Headteacher)

(Signed) ______________________________________
(Computing and Technology Coordinator)

Policy Date: November 2015
Review Date: November 2017