Nominated Lead Member of Staff: Pru Ashplant

Status & Review Cycle: Non-Statutory

St Jude's Church of England Schools Federation

E SAFETY POLICY

This school is committed to safeguarding and promoting the welfare of pupils and expects all staff and volunteers to share this commitment.

The e-safety policy relates to other policies including those for Use of ICT, anti-bullying and for child protection.

- The school has an e-safety co-ordinator (Pru Ashplant)
- Our e-safety policy has been written by the senior leadership team of the school, building on best practice and government guidance. It has been approved by governors.
- The e-safety policy and its implementation will be reviewed annually.

Teaching and Learning

Why 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.
- The school internet access is provided by Surrey County Council through a regional broadband contract, which includes filtering appropriate to the age of pupils.
- 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 safe, 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 appropriately to a wider audience.
- Pupils will be taught how to evaluate internet content
- The school will seek to ensure that the use of internet derived materials by staff and by 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.
- Pupils will be taught how to report unpleasant internet content e.g. using the CEOP ReportAbuse icon or Hector Protector.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Real-time virus protection and virus definition updates are continually in place via the Surrey preferred anti-virus and ransomware software, Sophos.
- Security advice is given when it is relevant, by the Local Authority.

E-mail

- Our pupils do not have school email accounts and therefore no communication between staff and pupils, via email, will take place.

Published content and the school website

- The contact details on the school website are the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility of the website and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not include any whose parents have not given permission.
- Pupils' full names will not be published on the website or on the school Twitter account.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or on the school Twitter account.

Social networking

- The school will control access to social networking sites. This control will mean that every site will be blocked as the recommended age for their use is 13 years.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform. (Wiki)
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of opportunities; however it does present dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work in partnership with Surrey County Council and our broadband supplier, RM Safety Net, to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety co-ordinator.
- Our IT partners and e-safety co-ordinator will make regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Mobile phones and associated cameras will not be used for personal reasons by staff or pupils during lessons or formal school time. In an emergency situation, when a member of staff must receive a call, they should leave the classroom.
- Staff will use a school phone where contact with pupils or parents is required.

- Whenever possible, staff must use a school allocated mobile device for taking photographs or videos on school trips or within school. Personal phones or devices may be used under the conditions explained in the staff Code of Conduct (p.10)

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the school's Data Protection policy.

Policy Decisions

Authorising internet access

- All staff must read and sign the 'Staff Code of Conduct' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents will be asked to sign and return a consent form.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Surrey CC can accept liability for the material accessed or any consequences of internet access.
- The school will monitor ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

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 school's complaints procedure, which can be found on the website.

Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

Communications

Introducing the e-safety policy to pupils:

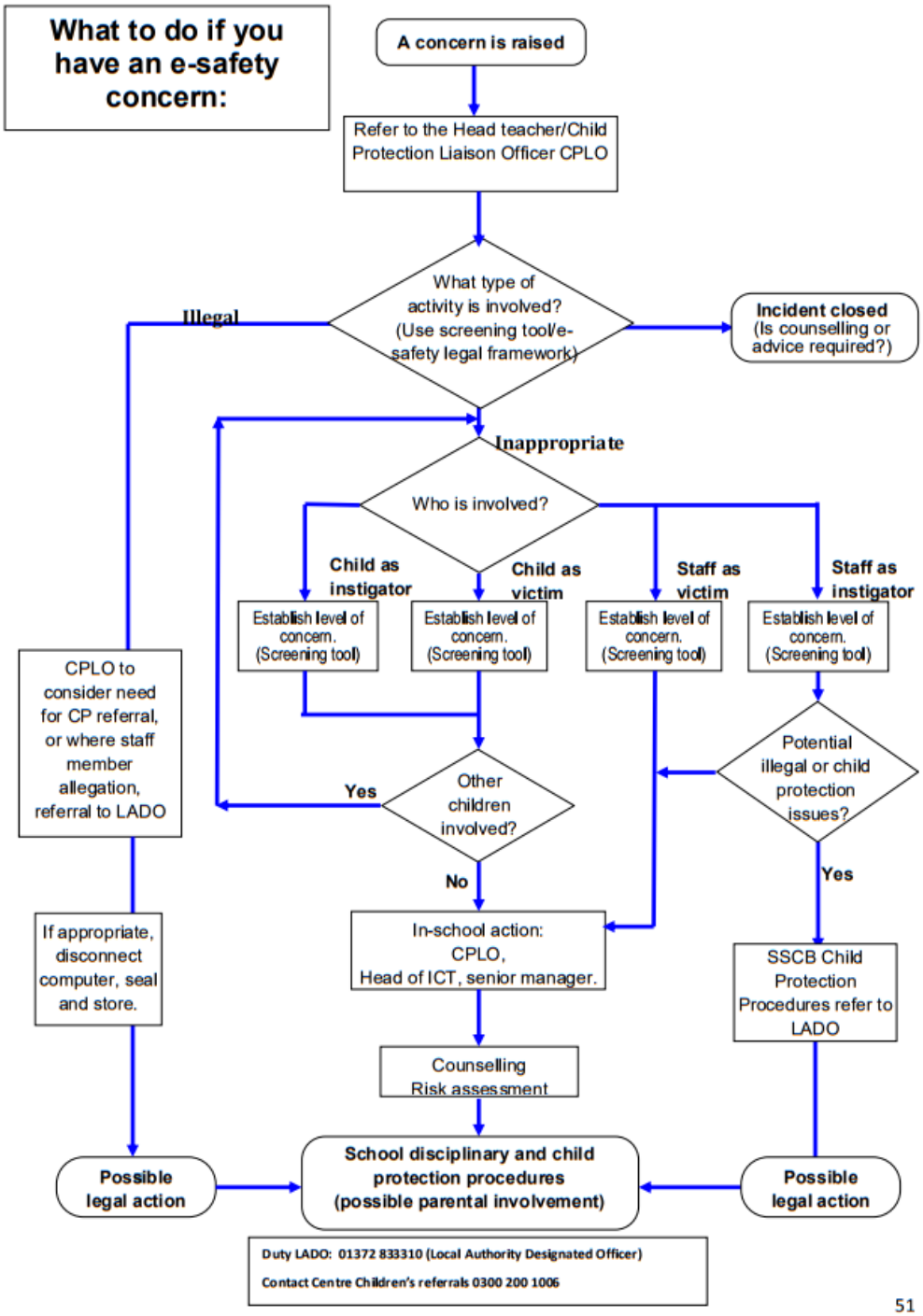
- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in the ICT suite.
- Pupils will be informed that network and internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils. This should be addressed each year as pupils become more mature and the nature of newer risks can be identified.

Staff and the e-safety policy

- All staff will be given the school e-safety policy and its importance explained.
- All staff will read the e-safety policy and agree to work within the guidelines.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the school e-safety policy in newsletters 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.
- Parents should be given e-safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.


What to do if you have an e-safety concern:
A concern is raised
Refer to the Head teacher/Child Protection Liaison Officer CPLO
What type of activity is involved? (Use screening tool/e-safety legal framework)
Illegal
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)
CPLO to consider need for CP referral, or where staff member allegation, referral to LADO
Other children involved?
Yes
No
Potential illegal or child protection issues?
Yes
If appropriate, disconnect computer, seal and store.
In-school action: CPLO, Head of ICT, senior manager.
SSCB Child Protection Procedures refer to LADO
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures (possible parental involvement)
Possible legal action
Duty LADO: 01372 833310 (Local Authority Designated Officer)
Contact Centre Children's referrals 0300 200 1006