St Ann's Heath Junior School

E-Safety Policy

This school is committed to safeguarding, child protection, and promoting the welfare of children and young people and expects all members of the school and its community to demonstrably share this commitment.

E-safety is part of the school's safeguarding responsibilities. The term e-safety can also be known as internet safety, online safety and web safety. Collectively these are defined as the safe and responsible use of technology.

Other related policies

This policy relates to other policies including those for child protection and safeguarding, behaviour, anti-bullying, acceptable use and pupil computer and safety rules.

Using this policy

- The school has an e-safety co-ordinator (Co-Head Teachers along with Computing Subject Lead)
- 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 every three years or as the need arises.
- The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.

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 RM and filtering is 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 taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- The school will seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught how to report unpleasant internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school uses a recognised internet service provider.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked by our ICT technician.
- The school will ensure that our networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems are in place to ensure that internet use can be monitored.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the class teacher who will then inform the e-safety co-ordinator.

Internet Use

- The school provides an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.
- Pupils will be advised not to give out personal details or information which may identify them or their location.

E-mail

- The school email system is run through Microsoft Office 365.
- The management of this system is the responsibility of the Computing Lead and ICT technician.
- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- No communication between staff and pupils, via email, should take place.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

Published content (school website, school social media accounts)

- The contact details are the school address, email and telephone number. Staff or pupil's 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 pupil's images and work

- Written permission will be obtained from parents or carers before photographs of pupils are published on the school website, the school Twitter account or any other school run social media.
- Photographs that include pupils will be carefully selected and will not include any whose parents have not given permission.
- Full names of pupils will not be published.

Social networking

- The school will control access to social networking sites.
- Pupils must not place personal photos on any social network space provided in school.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of opportunities, however it can present dangers for pupils.
- Pupils will be advised to use nicknames and avatars when using social network sites.
- Staff and pupils should ensure that their online activity, both in school and out, takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Managing emerging technologies

- Mobile phones and associated cameras will not be used by staff or pupils during lessons or formal school time.
- Staff will use a school phone where contact with pupils or parents is required.
- Whenever possible, staff must use a school allocated mobile device to taking photographs or videos on school trips or within school.
- Staff must not store images of pupils or pupils' personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices using in school or on school business.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the Data General Data Protection Regulations and the school's Data Protection Policy.

Policy Decisions

Authorising Internet Access

- All staff must read and sign the Acceptable Use Agreement and ICT Code of Conduct for Staff, Governors and Visitors 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 to allow use of technology by their child.

Assessing risk

- The school will take reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not always possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Surrey CC 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 by pupils will be dealt with by a senior member of staff. Any complaints 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 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 in the form of a Pupil Acceptable Use Policy.
- E-safety rules will be displayed in the ICT suite.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils.

To staff:

- All staff will be shown the e-safety policy and its importance explained.
- All staff must sign and agree with the Acceptable Use Agreement and ICT Code of Conduct for Staff, Governors and Visitors.

To parents:

- Parents' and carers' attention will be drawn to the e-safety policy in newsletters and on the school website.

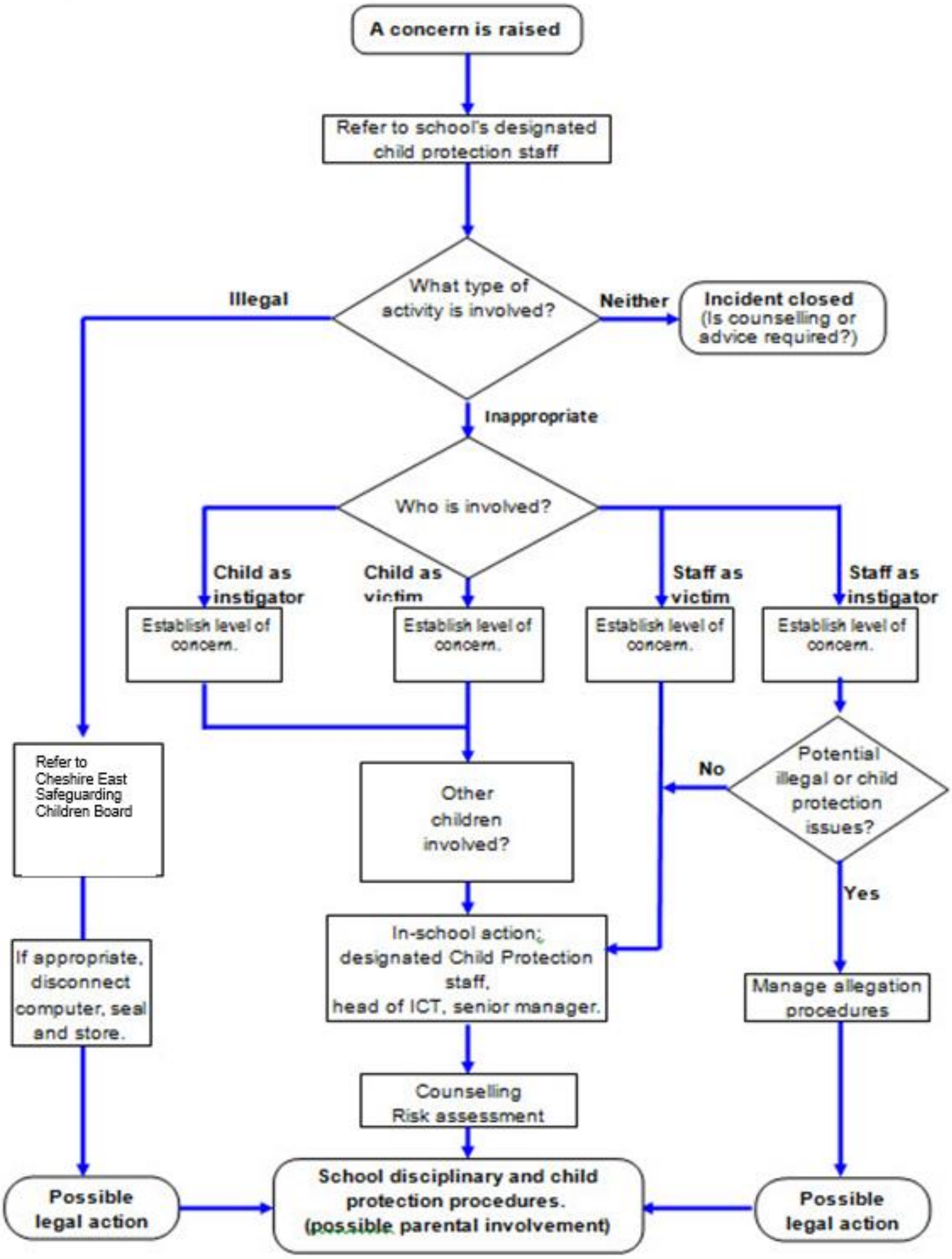
- Parents will be offered e-safety training every two years.

Monitoring and Evaluation

Implementation of this policy is monitored by the Headteacher and by governors through the Vision and Ethos Committee to evaluate its implementation and effectiveness. This policy will be reviewed by staff and governors every three years, or earlier if need arises. This policy will be promoted and implemented throughout the school.

Policy Status	
Agreed by Staff	October 2018
Agreed by Governors	October 2018
Next Review Date	September 2021

Appendix One: What to do if you have an e-safety concern


A concern is raised
Refer to school's designated child protection staff
What type of activity is involved?
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.
Establish level of concern.
Establish level of concern.
Establish level of concern.
Refer to Cheshire East Safeguarding Children Board
Other children involved?
Potential illegal or child protection issues?
No
Yes
If appropriate, disconnect computer, seal and store.
In-school action; designated Child Protection staff, head of ICT, senior manager.
Manage allegation procedures
Counselling Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action