POWELL CORDEROY SCHOOL
E-SAFETY POLICY

Last reviewed: June 2017

Due for review: Summer 2018

Owner: Computing Leader

Reviewed by: Full Governing Body

Review Status: Annual

E-safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for **behaviour, safeguarding, anti-bullying, data handling and the use of images, and the use of social media.**

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.

The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

1. Managing access and security

1.1. 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

1.2. The school will use a recognised internet service provider or regional broadband consortium.

1.3. The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.

1.4. The school will ensure that its networks have virus and anti-spam protection.

1.5. Access to school networks will be controlled by **personal** passwords.

1.6. Systems will be in place to ensure that internet use can be monitored and a log of

1.7. any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.

1.8. The security of school IT systems will be reviewed regularly.

1.9. All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.

1.9.1. Class teachers are responsible for monitoring the use of IT equipment and the internet, and reporting any issues to the IT technician via the log of concerns held in the IT technician's pigeon hole.

1.9.2. The IT technician is responsible for conducting weekly checks of the filtering system, and generating a weekly report to the Headteacher which will flag any issues or concerns. It is the Headteacher's responsibility to ensure any issues are addressed.

1.10. The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

2. Internet Use

2.1. The school will provide 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.

2.2. All communication between staff and pupils or families will take place using school accounts.

3. E-mail

3.1. Pupils and staff may only use approved e-mail accounts on the school IT systems

3.2. Staff to pupil email communication must only take place via a school email address or from within the learning platform.

3.3. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

3.4. E-mail from pupils to external bodies will be checked by teachers and only used as part of directed learning activities in school.

3.5. Teachers should not generally invite parents to email them directly. As a generic rule, all emails for teachers should be sent via info@pcps.uk marked FAO the teacher in question.

3.6. Where individual circumstances require a parent/teacher to email directly, teachers should ensure their line managers are aware and cc their line manager and/or headteacher (as most appropriate) if the nature of the correspondence is a complaint or of concern.

4. Published content eg school web site, school social media accounts

4.1. The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

4.2. The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

5. Publishing pupils' images and work

5.1. Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children.

5.2. Parents attending school events will be reminded that parental permission should be obtained before any photos including other people's children are shared online.

6. Use of social media including the school learning platform

6.1. The school has a separate social media policy which is owned by the Friends of Powell Corderoy School, who run a school-affiliated Facebook Page.

6.2. The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.

6.3. Use of video services such as Skype, Google Hangouts and Facetime will be controlled and monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.

6.4. Staff and pupils should use 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.

7. Use of personal devices

7.1. Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the e-safety policy and the relevant Acceptable Use of IT Policy.

7.2. Staff must not store images of pupils or pupil personal data on personal devices.

7.3. The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

7.4. Staff and pupils may not use personal devices in the classroom or school environment in the presence of other pupils, or during their working hours (i.e. staff may use personal devices in the staffroom during breaks, pupils may use them before and after school hours once they have left school.)

7.5. Handheld devices belonging to the school which may be mistaken for personal devices (e.g. classroom phones and ipads used for recording work) should be clearly externally marked with the school's names and/or logo.

8. Protecting personal data

8.1. The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

9. Policy Decisions

9.1. Authorising access

9.1.1. All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, IT technicians and governors) must read and sign the 'Staff Acceptable Use of IT' before accessing the school IT systems.

9.1.2. The school will maintain a current record of all staff and pupils who are granted access to school IT systems.

9.1.3. At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.

9.1.4. At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.

9.1.5. People not employed by the school must read and sign a Guest Acceptable Use of IT Policy before being given access to the internet via school equipment.

9.1.6. Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

9.2. 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 SCC can accept liability for the material accessed, or any consequences of internet access.

10. Handling e-safety complaints

10.1. Complaints of internet misuse will be dealt according to the school behaviour policy.

10.2. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures, with specific reference to the flowchart in Appendix 1 of this policy.

10.3. Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behavior policy.

11. Community use of the internet

11.1. Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

12. Communication of the Policy

12.1. To pupils

12.1.1. Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet

12.1.2. Pupils will be reminded about the contents of the AUP as part of their e-safety education

12.2. To staff

12.2.1. All staff will be shown where to access the e-safety policy and its importance explained.

12.2.2. All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet

12.2.3. All staff will receive e-safety training on an annual basis, usually during a staff meeting in e-Safety week. This is delivered by the school e-Safety Leader and based on most recent guidance from Childnet International (http://www.childnet.com/teachers-and-professionals/staff-e-safety-inset-presentation).

12.3. To parents

12.3.1. The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

12.3.2. Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school web site.

12.3.3. Parents will be offered e-safety training annually

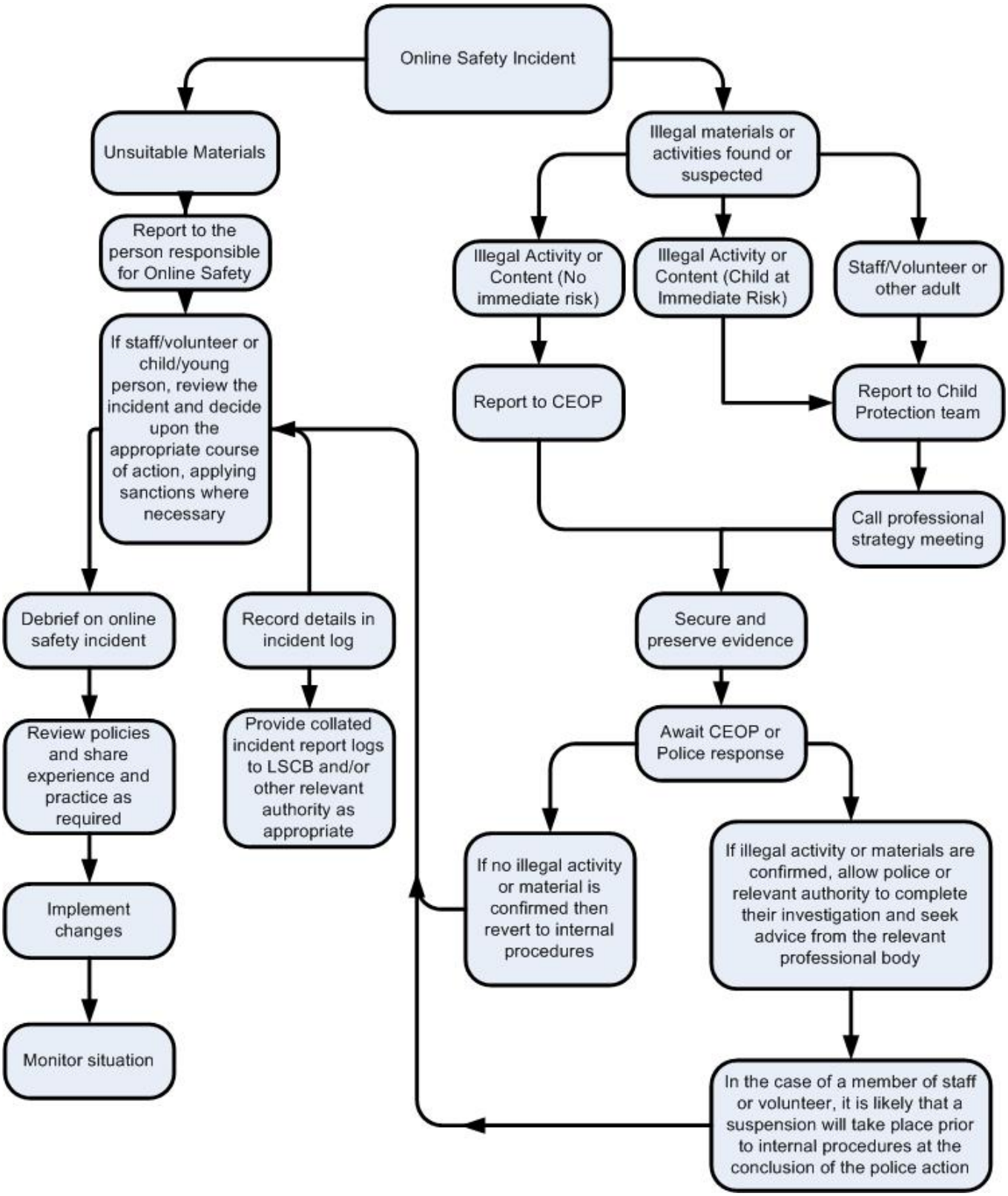
Policy approved by: _____ (print name)

On behalf of: _____ (committee or FGB)

Signed: _____

Date: _____

APPENDIX 1: Responding to an online safety incident


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action