Pallister Park Primary School E-Safety Policy

The Head Teacher and Governing body have a legal responsibility to safeguard children and staff and this includes online activity.

This document’s purpose is to outline the policy regarding the use of digital and electronic equipment that may potentially connect to the internet or for use within school. This will provide a basis to ensure pupils are ‘e-safe’ within Pallister Park School and any e-safety issues are reported and dealt with accordingly.

- The school has appointed an e–Safety Coordinator.
- The e–Safety Policy and its implementation will be reviewed annually.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors and other stakeholders such as the PTA.
- The School has appointed the lead responsibility for e-Safety to the Finance and Resource Committee

The School e-Safety Coordinators are **H Snowball** R **Leggott**

Policy approved by Head Teacher: **C Wain** Date: **10.09.18**

Policy approved by Governing Body: **R Brown** (Chair of Governors) Date: **14.10.15**

The date for the next policy review is October 2019

Table of Contents

1.2 Teaching and learning

1.2.1 Why is Internet use important?

Internet use within school and using school equipment outside of school by staff and pupils will recognise the following guidelines:

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday 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.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

1.2.3 How can Internet use enhance learning?

Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others digitally.

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 How will pupils learn how to evaluate Internet content?

Pupils will be made aware that not everything on the internet is accurate information.

- 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 use age-appropriate tools to research Internet content.

1.3 Managing Information Systems

1.3.1 How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.

1.3.3 How will published content be managed?

Due to the nature of published content on the internet this must be treated appropriately.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

- Staff publishing material to the schools social media channels will ensure that it is appropriate and follows the guidelines set out in this document and the acceptable use policy.

1.3.4 Can pupils’ images or work be published?

Prior consent is required to use pupils images including consideration for the following:

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils’ full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Changes in circumstance of parents/carers for a pupil will be recognised by the parents/carers, should the written permission for images/videos wish to be changed.

1.3.5 How will social networking, social media and personal publishing be managed?

Staff should be aware that, when communicating via social networking sites, anything said, shown or received could potentially be made available to a wider audience than originally intended.

- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- Staff must not contact pupils on social networking sites, this includes any child who attended the school previously but is under that age of 18 years.
- Should a member of staff receive messages on their social networking profile, which they suspect is from a pupil, they must report this to the Head Teacher, who will decide the appropriate action.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff must not disclose, on any social networking site, any information that is confidential to the school or governing body, or information about a colleague or pupil.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

1.3.6 How will filtering be managed?

The school has implemented an internet filtering system to provide safety to pupils and staff online, it is recognised that this will not always be 100% effective and a clear line channel is available for reporting and recording any incidents that may occur.

- The school will work with OneIT and Council to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. *See Appendix 'e-Safety incident flowchart'*
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Cleveland Police or CEOP

1.3.8 How are emerging technologies managed?

The school will keep up to date with new technologies and adapt this document should it be deemed necessary to incorporate any additional e-safety concerns.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

1.3.9 How should personal data be protected?

Personal data will be backed up regularly by the appropriate IT Support staff, this may be a contracted third party.

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

1.4 Policy Decisions

1.4.1 How will Internet access be authorised?

Unless specifically denied all pupils and staff will have internet use in the school.

- The school will maintain a current record of all staff and pupils who are granted access to the school’s electronic communications.
- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.

1.4.2 How will risks be assessed?

The school will take reasonable measures to protect pupils activities using ICT equipment.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- Methods to identify, assess and minimise risks will be reviewed regularly.

1.4.3 How will the school respond to any incidents of concern?

- E-safety incidents will be responded to according to the ‘e-Safety incident flowchart’. *(See appendix)*

1.4.4 How will e–Safety complaints be handled?

Parents, teachers and pupils will be aware of how to report an e-safety incident, the e-Safety incident flowchart will be made available to provide a clear channel of communication should any incidents occur.

- Complaints about Internet misuse will be dealt with under the School’s complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- All members of the school will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

1.4.6 How will Cyberbullying be managed?

Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

1.4.7 How will Learning Platforms be managed?

Learning Platforms (LP) use in the school will be subject to the following guidelines:

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

1.4.8 How will mobile phones and personal devices be managed?

Use of digital equipment within school and the responsibility of the school in managing these devices and their access to school systems and the internet is outlined below:

- The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use or Mobile Phone Policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.

- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.

- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student’s withdrawal from either that examination or all examinations.

- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

- Staff will be issued with a school phone where contact with pupils or parents/carers is required.

- Mobile Phone and devices will be switched off or switched to ‘silent’ mode, Bluetooth communication should be “hidden” or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

1.5 Communication Policy

1.5.1 How will the policy be introduced to pupils?

Implementation of the e-safety policy will be managed in a way to engage the pupils and increase their awareness of relevant items within the policy and any concerns they should have regarding their internet access within the school.

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.

1.5.2 How will the policy be discussed with staff?

Staff will be made aware of the e-safety policy and its contents, in particular the ‘e-Safety incident flowchart’ so they are aware of potential issues and clear lines of communication in reporting and recording these incidents.

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement an Acceptable Use Policy.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Reference documents

Schools e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

Has the school an e-Safety Policy that complies with Kent guidance?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N

Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y/N
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/carers or pupils sign an Acceptable Use Policy?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N
Does the school log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

‘e-Safety incident flowchart’ reference sites:

- **Childrens Safeguarding unit:** http://www.middlesbrough.gov.uk/MSCB/safeguarding
- **One IT Helpdesk:** https://helpdesk.oneitss.org.uk/
- **Internet Watch Foundation**: http://www.iwf.org.uk
- **Cleveland Police**: http://www.cleveland.police.uk/

Kidsmart: www.kidsmart.org.uk

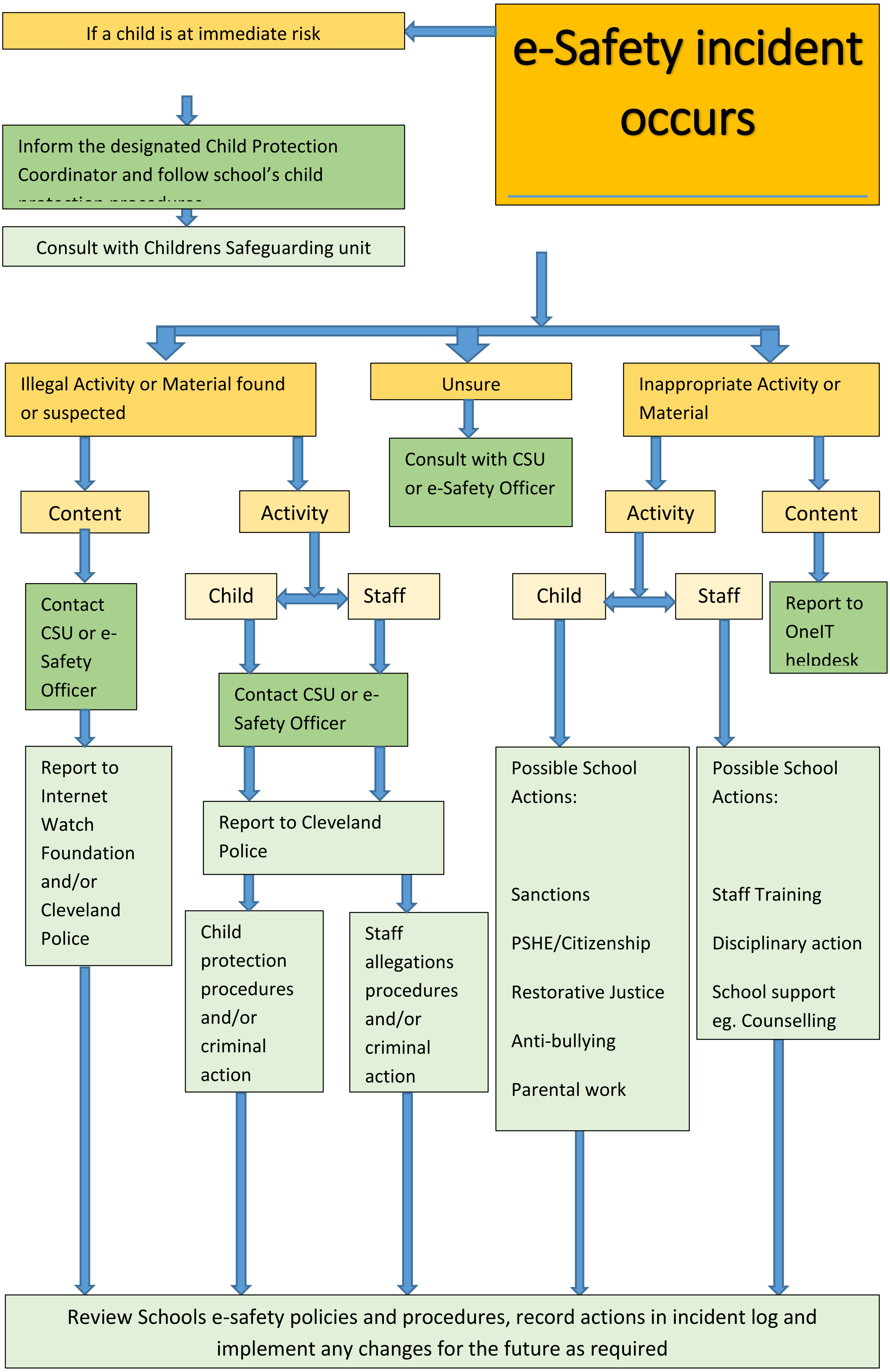
Schools e–Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

e-Safety incident flowchart


e-Safety incident occurs
If a child is at immediate risk
Inform the designated Child Protection Coordinator and follow school's child protection procedures
Consult with Childrens Safeguarding unit
Illegal Activity or Material found or suspected
Unsure
Inappropriate Activity or Material
Consult with CSU or e-Safety Officer
Content
Activity
Activity
Content
Contact CSU or e-Safety Officer
Child
Staff
Child
Staff
Report to OneIT helpdesk
Contact CSU or e-Safety Officer
Report to Internet Watch Foundation and/or Cleveland Police
Report to Cleveland Police
Possible School Actions:
Sanctions
PSHE/Citizenship
Restorative Justice
Anti-bullying
Parental work
Possible School Actions:
Staff Training
Disciplinary action
School support eg. Counselling
Child protection procedures and/or criminal action
Staff allegations procedures and/or criminal action
Review Schools e-safety policies and procedures, record actions in incident log and implement any changes for the future as required