PASHLEY DOWN
INFANT SCHOOL

ONLINE SAFETY POLICY

REVIEWED JULY 2017
DATE FOR REVIEW JULY 2020

ONLINE POLICY

1. Rationale

1.1 New technologies have become integral to the lives of children in today's society, both within school and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and children to learn in new ways

1.2 The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents / carers, members of the school community and the children themselves.

1.3 The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the use of these new technologies can put children at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The risk of radicalisation and involvement in hate crime *(see Prevent policy)*
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the child.

1.4 Many of these risks reflect situations in the off-line world and it is essential that this online safety policy issued in conjunction with other school policies *(eg behaviour, anti-bullying safeguarding and child protection).* As with all other risks, it is impossible to eliminate those risks completely. Therefore, it is that we aim to protect children, and to build their confidence and skills in dealing with the risks associated with the on-line world, so that they can feel safe.

1.5 The school aims to implement safeguards to help keep children safe. The school will do everything that could reasonably be expected to manage and reduce the risks associated with the internet and new technologies.

1.6 This online safety policy explains how we intend to do this, while also addressing wider educational issues in order to help children and their parents / carers to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Development of the Policy

This online safety policy has been developed through consultation with staff, governors, parents / carers and children. The consultation has taken place in staff meetings, governor meetings, meetings with parent representatives and School Council meetings.

3. Monitoring and Review of the Policy

3.1 The monitoring of this online safety policy will be undertaken by the Online safety co-ordinator, Senior Management Team and Computing Curriculum Leader (some of these roles may overlap). Monitoring and review will take place at regular intervals. This policy will be updated in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place

3.2 Should a serious online safety incident occur, the Safeguarding Officer should be informed, and their advice followed. *(see Appendix 1)*

3.3 The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Notes of concerns raised by children, parents / carers and staff

4. Scope of the Policy

4.1 This policy applies to all members of the school community (including staff, children, volunteers, parents / carers, visitors) who have access to, and are users of, the school ICT system.

4.2 We recognise that Infant-aged children are very unlikely to use technology in a harmful way outside of school (for example, cyberbullying). However, it must be noted in this policy that the Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour that harms a member of the school. Again, it is unlikely that there would be a need to take such

action and the school would work closely with parents / carers in dealing with matters of online safety.

5. Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

5.1 **Governors** are responsible for the approval of the online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors undertaking visits, which will include speaking to children. A member of the Governing Body has taken on the role of online safety Governor. Should there be any online safety incidents, these would be reported to the online safety Governor; this governor will report to the relevant committee. The Online safety Governor will also assist the Online safety Coordinator with the monitoring of the school online safety policy.

5.2 The **headteacher** is responsible for ensuring the safety of members of the school community, including online safety, and so will be the online safety Co-ordinator. The online safety Co-ordinator ensure that there are procedures in place to be following in the event of a serious online safety incident.

5.2.1 The **online safety Co-ordinator** will:

- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- liaise with the Local Authority
- liaise with school ICT technician
- attend relevant meeting / committee of Governors
- ensure that there is a system in place to allow for monitoring online safety
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place

5.2.2 The headteacher is also the main **designated person for child protection**, and so will be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

5.3 The **ICT Technician** is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Online safety guidance

- that users may only access the school's networks through a properly enforced password protection policy
- that he keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

5.3 The **children** are responsible for using the school ICT systems in accordance with the rules for pupils outlined in the Internet Acceptable Use Policy. These rules help children to understand how to keep safe when using ICT *(see Internet Acceptable Use policy).*

5.4 **Parents / Carers** play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will help parents and carers to understand these issues through Forum evenings, newsletters, the school website, local online safety campaigns and literature. Parents and carers will be responsible for following the Internet Acceptable Use policy.

6. Staff and governor Training

6.1 It is important that staff need to understand their responsibilities, as outlined in this policy, and so the following training will be offered:

- Staff knowledge will be updated regularly through the programme aimed a promoting children's safety. All relevant policies will be discussed on an annual basis. Where staff have individual training needs, this will be addressed through the performance management process.
- All new staff will receive induction information, which will include reference to all key policies *(including Online safety policy, Internet Acceptable Use policy and Child Protection policy).*
- The Online safety Coordinator will keep up-to-date on Local Authority advice through Czone and advice newsletters.
- attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA / LA and others.
- The Online safety policy will be presented to, and discussed by, staff in meetings. (May 2017)
- The Online safety Coordinator and IT technician will provide advice and guidance to individuals as required

6.2 As governors also have responsibilities in connection with online safety, training will be offered to enable them to fulfil their role. Training is of particular importance for those who are members of any committee involved in ICT, online safety, health and safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation *(the school buys into the Services to Schools package that*

provides governor training – either for individual governors, or the Full Governing Body).

- Participation in school training or information sessions for staff or parents

7. Educating children about Online safety

7.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in online safety is therefore an essential part of the school's approach to keeping children safe. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety education will be provided in the following ways:

- Teachers will provide termly online safety lessons, as part of the work in computing – this will cover the use of ICT and new technologies in school and outside school. This aspect of learning will be regularly revisited. (See Scheme of work for computing)
- In lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that the teacher has thought through ways of dealing with any unsuitable material that may appear when children undertake internet searches (*blocking software reduces, but cannot totally eliminate this possibility)* - for example, teaching the children to click on the 'dolphin'.
- As appropriate to the age and level of understanding, teachers will teach children to be critically aware of the materials they access on-line – and to question the accuracy of the information *(i.e. the content may not be correct, the source may not be reliable).*
- Teachers will teach children to respect copyright when using material on the internet.
- Rules for use of use of computers, and safe use of the internet, will be displayed.
- Teachers will monitor use of computers in the suite using the desktop overview' software. In classrooms, computer will be positioned so that teachers and TAs have a good view of the screen.
- Children will not be given individual school email address – only school / class email addresses will be used. Teachers will compose email messages sent by the class, with the input of the children. Teachers will use this modelling as a way of teaching children how to write emails in a correct manner - whilst also teaching them what NOT to do *(for example sending angry, bullying or upsetting messages*).
- Although children will not use individual emails at school, they may do so at home. Therefore, teachers will teach children about email safety issues, such as the risks attached to the use of personal details. Teachers will also teach children how to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

7.2 All parents / carers have an essential role in teaching their child/ren online safety at home, and in monitoring and regulating their child/ren's use of ICT. However, some parents / carers may have only a limited understanding of online safety issues, and the risks to their child/ren. The school will support parents in their role of keeping children 'e-safe' at home, by providing information and by raising awareness, through Forum evenings, letters, newsletters and the school website.

9. Use of digital and video images - Photographic, Video

9.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have created or downloaded from the internet. However, staff and children need to be aware of the risks associated with sharing images, and with posting digital images on the internet. Those images may remain available on the internet forever and may have the potential to cause harm or embarrassment to individuals in the short or longer term *(for example, there are many reported incidents of employers carrying out internet searches for information about potential and existing employees) See Digiduck story App on I Pads*

9.2 The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet *eg on social networking sites.*
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Photographs should only be taken on school equipment; the personal equipment of staff should <u>not</u> be used for such purposes.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without the permission of their teacher.
- Photographs published on the website (or elsewhere) that include children will be selected carefully and will comply with good practice guidance on the use of such images. *(also see next point).*
- Children's full names will not be used anywhere on a website. Children's names will not be published in association with photographs. Parents / carers have the right to request that their child's image should NOT be published (on the school website, or in other publications such as the local paper).

8. Technical – infrastructure / equipment, filtering and monitoring

8.1 The school will take all reasonable and practicable measures to ensure that the school infrastructure / network is as safe and secure, and that the policies and procedures within this policy are implemented. This will include:

- Managing the school ICT systems in ways that ensure that they meet the online safety technical requirements outlined by the Local Authority
- Regular reviews of the safety and security of the school ICT system
- Ensuring that servers, wireless systems and cabling are securely located and that physical access is restricted
- Supporting the managed filtering service provided by RM – and reporting any filtering issues to RM.
- Taking appropriate security measures to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Ensuring that the school infrastructure and individual workstations are protected by up to date virus software.
- Ensuring that all users will have clearly defined access rights to school ICT systems.

8.2 The school managers will also take all reasonable measures to ensure that staff carry out their online safety responsibilities in keeping the system safe. Staff will:

- Be responsible for the security of their username and password – they will not allow other users to access the systems using their log on details and they must immediately report any suspicion of a breach of security.
- Report to the Computing Curriculum Leader, any websites that that they feel should be removed from the filtered list *(e.g. sometimes educational websites are blocked).* The Computing Curriculum Leader will consider the request, and will consult the headteacher. If the request is agreed, the Computing Curriculum Leader will record this in a log, which will be reviewed regularly by the Online safety governor and/or relevant governor committee.
- Report to the Computing Curriculum Leader or Online safety Co-ordinator, any actual or potential online safety.
- Ensure that family members do not use school equipment (e.g. school laptops or other portable devices that are being used by the staff member to do work at home).
- Follow the policy of only <u>secure</u> removable media devices (eg memory sticks) on school computers.
- *Not* send personal data over the internet, or take data off the school site unless it has been safely encrypted or otherwise secured.
- *Not* download programmes or Apps onto school laptops or other portable devices (e.g. iPad, iPods). IT technician will download any suitable Apps

9. Data Protection

9.1 The school has a Data Protection policy, which follows the requirements set out in the Data Protection Act 1998. In summary, this policy states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

9.2 Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. In relation to online safety, this means that staff must ensure that they:

- Take care, at all times, to ensure the safe keeping of personal data saved on computers, on other devices and on the school or other networks – to minimise the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
  - the device must offer approved virus and malware checking software
  - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

10. Communications

10.1 One of the key advantages of new technologies is the way it opens up new methods of communication, and it is recognise that communications technologies have the potential to enhance learning. However, technology also increases the possibility of harm, through inadvertent or deliberate misuse. To mininize the risks the following table sets out for staff, how these devices may be used:

	Allowed	Only allowed *(outside school)* if there is NO mention of school	Not allowed
Staff bringing Mobile phones into school	✓		
Use of mobile phones in lessons (conversations or texting)			✓

Taking photos on mobile phones			✓
Use of mobile phones in social time	✓		
Use of school email for personal emails			✓
Use of chat rooms		✓	
Use of social networking sites		✓	
Use of blogs		✓	

10.2 When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure.
- Only official school email addresses should be used to communicate with members of staff, and school contacts, partner agencies
- Users need to be aware that email communications may be monitored.
- Users must immediately report to Senior Managers, any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Staff must take care not to respond to any such email.
- Any digital communication between staff and parents / carers *(e.g. email)* must be professional in tone and content. Note: Class staff must be extremely careful about using digital communication with parents or children. It is always preferable to use other methods *(e.g. face-to-face, notes or letters).* Where a teacher or TA feels that they must communicate via email, they should discuss this with a Senior Manager, and copy the headteacher into any email correspondence. *For advice on using other forms of digital communications, please see the Social Media policy.*
- Staff should NOT use any form of digital communication technology to correspond / chat to children.
- Personal information will not be posted on the school website, unless chosen to do so.

11. Unsuitable / inappropriate activities

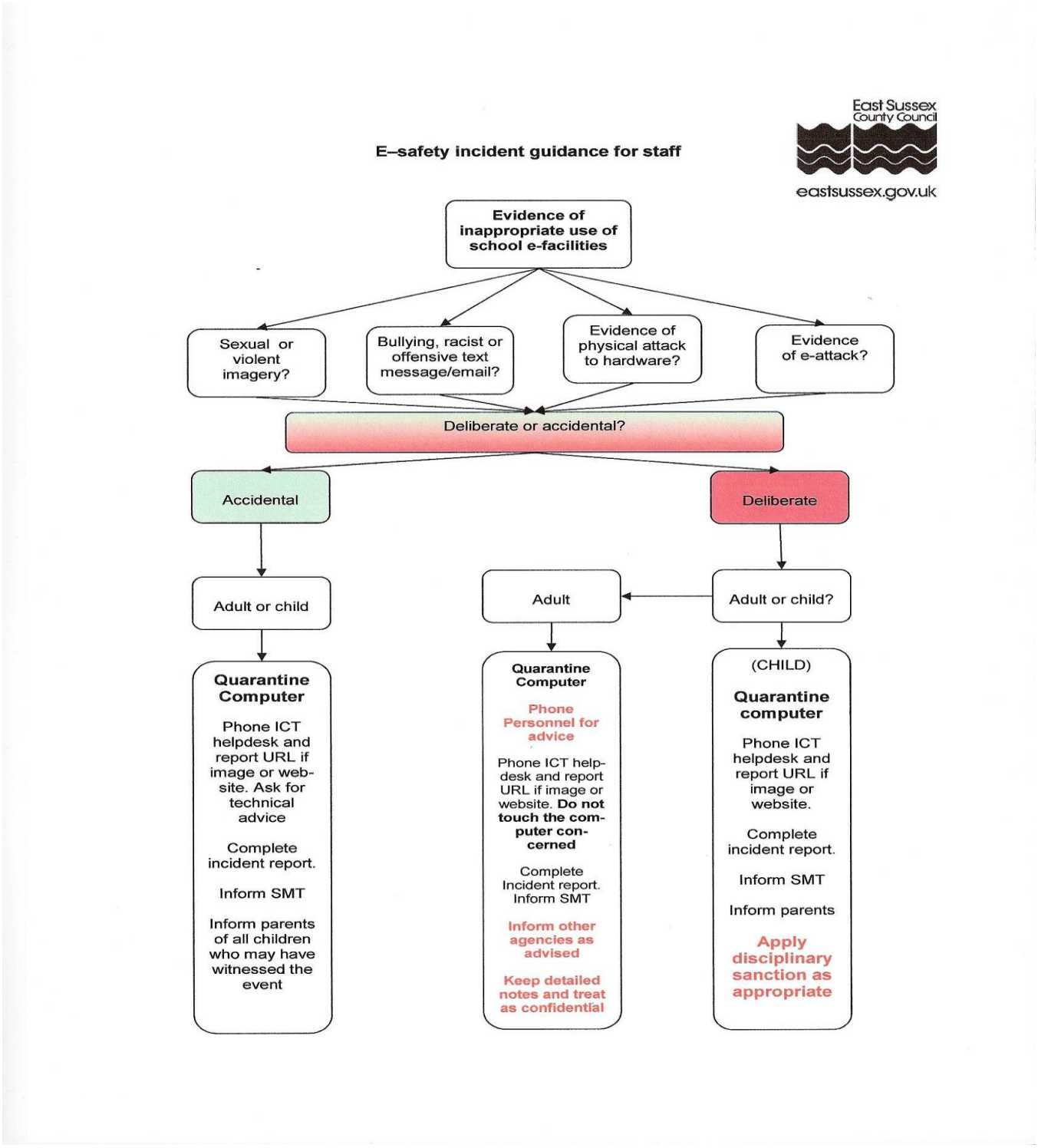
11.1 Some internet activity *eg accessing child abuse images or distributing racist material* is illegal and is obviously be banned from the school and all other ICT systems. Any type of illegal activity could lead to criminal prosecution. Other activities *eg Cyber-bullying* are against the ethos of the school, and would result in disciplinary action, as would any action which goes against the guidelines set out in this policy.

11.2 There are also other activities that may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

11.3 The table below set out the school policy for a range of internet activities, and should be followed by all members of the school community *(staff, governors, parents / carers, students, volunteers and children)* when using school equipment or systems (inside or outside school). The school policy restricts certain internet usage as follows:

Activity	Acceptable	Acceptable at certain times	Unacceptable and illegal
Child sexual abuse images			✓
Promotion or conduct of illegal acts e.g. under the child protection, obscenity, computer misuse and fraud legislation			✓
Adult material that potentially breaches the Obscene Publications Act in the UK			✓
Post, download, upload, transfer, communicate or pass on criminally racist material, pornography of any kind of discriminatory material			✓
Comments that contain or relate to any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school, or brings the school into disrepute			✓
Using school systems to run a private business			✓
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by RM or the school			✓
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions			✓
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)			✓
Creating or propagating computer viruses or other harmful files			✓
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet			✓
On-line gaming (educational)		✓	
On-line gaming (non educational)			✓
On-line gambling			✓
On-line shopping / commerce *(<u>Office only</u> – following finance guidelines)*		✓	
File sharing		✓	
Use of social networking sites *(NOTE: see guidelines in this policy and the Social Media policy)*		✓	
Use of video broadcasting *eg YouTube*		✓	

Appendix 1


E–safety incident guidance for staff
East Sussex County Council
eastsussex.gov.uk
Evidence of inappropriate use of school e-facilities
Sexual or violent imagery?
Bullying, racist or offensive text message/email?
Evidence of physical attack to hardware?
Evidence of e-attack?
Deliberate or accidental?
Accidental
Deliberate
Adult or child
Adult
Adult or child?
Quarantine Computer
Phone ICT helpdesk and report URL if image or web-site. Ask for technical advice
Complete incident report.
Inform SMT
Inform parents of all children who may have witnessed the event
Quarantine Computer
Phone Personnel for advice
Phone ICT help-desk and report URL if image or website. Do not touch the com-puter con-cerned
Complete Incident report. Inform SMT
Inform other agencies as advised
Keep detailed notes and treat as confidential
(CHILD)
Quarantine computer
Phone ICT helpdesk and report URL if image or website.
Complete incident report.
Inform SMT
Inform parents
Apply disciplinary sanction as appropriate

Appendix 2

Online safety Incident Record

Online safety incident		**Date:**		**Time:**	
Name of member of staff (Discovering the incident)					
Child(ren) involved. (Or other adults if no children involved)					
Nature of incident	Accidental access to inappropriate material	Intentional access to inappropriate material	Cyber Bullying	Grooming	Other
Details					
The event occurred	During a lesson	In unsupervised time	Outside school hours		
Does the event warrant direct Police involvement (YES if…)	Grooming	Violent images	Pornographic image(s)	Other criminal activity	

Headteacher / Deputy					
(Staff)	Personnel Contact made with	Recommended action	Action applied	Chair of Governors	
Other					
Children	Contacted Parents	Date		Time	

Interviewed Parents/Carers (Append *confidential* notes of interview)				
Name/s				
File FOUR copies:	Top Copy to HT	Second Copy to Child Safety Officer / ESCC	Third Copy to Child's file	Fourth copy to Staff member's Personnel file
Tick when done				

Appendix 3

PASHLEY DOWN INFANT SCHOOL

Online safety Log Book *(Activation of Hector)*

Date	Year group/Class/Child	Website address (Cut and paste this from Web address bar) Include a brief description of what was on screened or heard.	Reported to: JC	Action taken by JC/PF	Parent/carers informed