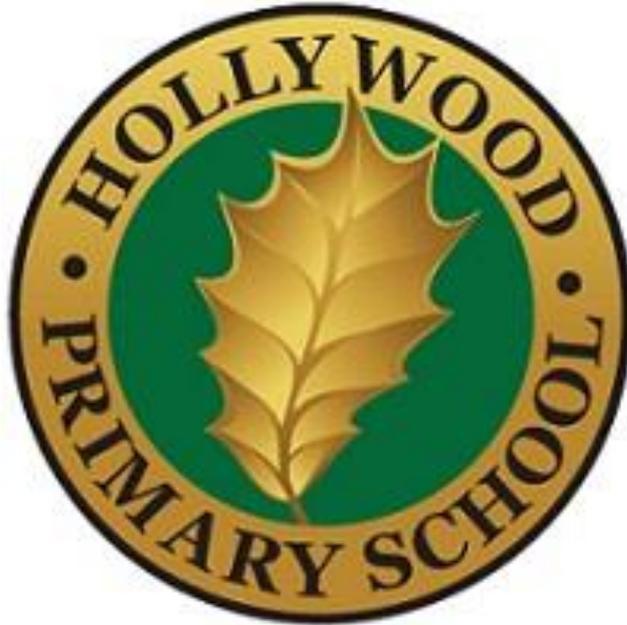


# HOLLYWOOD PRIMARY SCHOOL

## INTERNET SAFETY POLICY



### **Policy and Procedure: E Safety Policy**

Author:

Date:

Checked by:

Date of Governing Body approval:

Review date:

## E Safety Policy

### Contents

0. Introduction.....	2
1. Teaching and Learning .....	3
2. Managing Internet Access .....	5
3. Policy Decisions .....	10
4. Pupil Online Safety Curriculum .....	11
5. Communications Policy .....	14
Appendix 1 .....	15
Appendix 2 .....	17
Appendix 3 .....	19
Appendix 4 .....	20
Appendix 5 .....	22
Appendix 6 .....	23
Appendix 7 .....	24

## 0. Introduction

Protecting young people and adults properly means thinking beyond the Hollywood environment. Broadband, Wifi and 3/4G connections now mean the World Wide Web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in Hollywood or at home, their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

As a result, designing and implementing an e-safety policy demands the involvement of a wide range of interest groups: the Headteacher, Governors, Leadership Team, SENCO, Designated Safeguarding Lead, classroom teachers, support staff, young people, parents or carers, Local Authority personnel, Internet service providers (ISP), and Regional broadband consortia, working closely with ISPs on network security measures.

E-safety is a child protection issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

An e-safety policy should:

- allow young people to develop their own protection strategies for when adult supervision and technological protection are not available;
- give information on where to seek help and how to report incidents;
- help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the Hollywood will impose if they act inappropriately when online;
- provide guidelines for parents, carers and others on safe practice;
- ensure you regularly monitor and review your policies with stakeholders;
- ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety program.

Above all, e-safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

(<http://schools.becta.org.uk>)

**The purpose of this policy is to:**

- set out the key principles expected of all members of the community at Hollywood with respect to the use of IT-based technologies.
- safeguard and protect the children and staff of Hollywood.

- assist Hollywood staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as online bullying which are cross referenced with other Hollywood policies.
- ensure that all members of the Hollywood community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

## **1. Teaching and Learning**

### **1.1 Why the Internet and digital communications are important**

- The Internet is an essential element in 21st century life for education, business and social interaction. Hollywood 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.
- Teachers plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Staff model safe and responsible behaviour in their own use of technology during lessons.
- Teachers remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout Hollywood will be displayed when a student logs on to the Hollywood network.

### **1.2 Internet use will enhance learning**

- The Hollywood Internet access will be designed expressly for pupil use and will include 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 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 to a wider audience.

### **1.3 Pupils will be taught how to evaluate Internet content**

- Hollywood will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.

- Pupils will be taught how to report unpleasant Internet content to the appropriate person (DSL/Computing Lead/Class Teacher). This can be done anonymously, or in person, and will be treated in confidence.
- Hollywood has a clear, progressive Online safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
  - ✓ to STOP and THINK before they CLICK
  - ✓ to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - ✓ to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - ✓ to know how to narrow down or refine a search;
  - ✓ [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - ✓ to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - ✓ to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - ✓ to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - ✓ to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - ✓ to understand why they must not post pictures or videos of others without their permission;
  - ✓ to know not to download any files – such as music files - without permission;
  - ✓ to have strategies for dealing with receipt of inappropriate materials;
  - ✓ [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
  - ✓ To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
  - ✓ To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

## **2. Managing Internet Access**

### **2.1 Information system security**

- Hollywood ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

### **2.2 E-mail**

- Pupils may only use approved e-mail accounts on the Hollywood system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The Hollywood should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Hollywood Primary School:
  - ✓ Provides staff with an email account for their professional use (Microsoft 365) and makes clear personal email should be through a separate account.
  - ✓ Does not publish personal e-mail addresses of pupils or staff on the Hollywood website.
  - ✓ Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
  - ✓ Will ensure that email accounts are maintained and up to date
  - ✓ Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
  - ✓ Knows that spam, phishing and virus attachments can make e mails dangerous.

### **2.3 Published content and the Hollywood website**

- Staff or pupil personal contact information will not be published. The contact details given online should be the Hollywood office.
- The Headteacher/Deputy Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers.
- The Hollywood web site complies with the statutory DfE guidelines for publications.
- Most material is the Hollywood's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the Hollywood address, telephone number and we use a general email contact address, e.g. enquiry@hollywood.bham.sch.uk. Home information or individual e-mail identities will not be published.
- Photographs published on the web do not have full names attached.

- We do not use pupils' names when saving images in the file names or in the tags when publishing to the Hollywood website.
- We expect teachers using Hollywood approved blogs or wikis to password protect them and run from the Hollywood website.

## **2.4 Publishing pupil's images and work**

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on the Hollywood Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the Hollywood Web site.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the Hollywood policy on image taking and publishing, both on Hollywood and independent electronic repositories.
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the Hollywood agreement form when their daughter / son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published Hollywood produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the Hollywood web site, in the prospectus or in other high profile publications, Hollywood will obtain individual parental or pupil permission for its long term use.
- Hollywood blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

## **2.5 Social networking and personal publishing**

- Hollywood will control access to social networking sites, and consider how to educate pupils in their safe use.

- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside Hollywood brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' children from viewing their private pages.
- Staff will be shown how to 'block' their profile picture from being downloaded, and protect their profile information.
- Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the Hollywood preferred system for such communications.
- Hollywood staff will ensure that in private use:
  - ✓ No reference should be made in social media to students / pupils, parents / carers or Hollywood staff
  - ✓ They do not engage in online discussion on personal matters relating to members of the Hollywood community
  - ✓ Personal opinions should not be attributed to Hollywood or local authority
  - ✓ Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

## **2.6 Managing filtering**

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety lead/DSL.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## **2.7 Managing videoconferencing & webcam use**

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised.

## **2.8 Managing emerging technologies**

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

- The Senior Leadership Team should note that technologies such as mobile phones with wireless Internet access can bypass Hollywood filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Staff will not use personal mobile phones to communicate with children, or use them to capture images of them.

## **2.9 Protecting personal data**

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

## **2.10 Personal devices and mobile phones**

- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded.
- Hollywood reserves the right to search the content of any mobile or handheld devices on the Hollywood premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the Hollywood office to answer on their behalf, or seek specific permissions to use their phone at other than their break times. Mobile phones will not be used during lessons or formal Hollywood time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal Hollywood time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to Hollywood are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the Hollywood site.
- The Bluetooth or similar 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.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- Any permitted images or files taken in Hollywood must be downloaded from the device and deleted in Hollywood before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the Hollywood policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for Hollywood duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a Hollywood mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a School-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Students' use of personal devices
  - ✓ Hollywood strongly advises that student mobile phones should not be brought into school. However, we accept that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
  - ✓ If a student breaches the Hollywood policy then the phone or device will be confiscated and will be held in a secure place in the office. Mobile phones and devices will be released to parents or carers in accordance with the policy.
  - ✓ If a student needs to contact his or her parents or carers, they will be allowed to use a Hollywood 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 personally-owned devices and will be made aware of boundaries and consequences.
  - ✓ No students should bring his or her mobile phone or personally-owned device into Hollywood without teacher knowledge. All devices must be switched off and the "safe place" allocated.

### **3. Policy Decisions**

#### **3.1 Authorising Internet access**

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any Hollywood ICT resource. (See Appendix 4)
- Hollywood will maintain a current record of all staff and pupils who are granted access to Hollywood ICT systems.
- At EYFS and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the Hollywood will be asked to sign an "acceptable use of Hollywood ICT resources" before being allowed to access the internet from the Hollywood site. (See Appendix 4)

#### **3.2 Assessing risks**

- Hollywood will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Hollywood network. Neither the Hollywood nor Birmingham LA can accept liability for any material accessed, or any consequences of Internet access.
- Hollywood should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

#### **3.3 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 /Deputy Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with Hollywood child protection procedures. (See Appendix 3)
- Pupils and parents will be informed of the complaints procedure (see school's complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

#### **3.4 Community use of the Internet**

Hollywood will liaise with local organisations to establish a common approach to e-safety, if necessary.

## **4. Pupil Online Safety Curriculum**

### **4.1 Teaching and learning**

This school has a clear, progressive Online safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, including:

- ✓ to STOP and THINK before they CLICK
  - ✓ to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - ✓ to know how to narrow down or refine a search (KS2);
  - ✓ to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - ✓ to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - ✓ to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - ✓ to have strategies for dealing with receipt of inappropriate materials;
  - ✓ to understand why and how some people will 'groom' young people for sexual reasons (KS2);
  - ✓ to understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
  - ✓ to know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Teachers plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
  - School will remind students about their responsibilities through a Pupil Acceptable Use Policy (Appendix 5) which every student will sign.
  - All staff will model safe and responsible behaviour in their own use of technology during lessons.

### **4.2 Online risks**

- Hollywood recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

### **4.3 Cyber-bullying and abuse**

- 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
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with Hollywood / LA child protection procedures.
- Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful e-mails or text messages.
- Posters providing information about how to get help from ChildLine, ThinkUKnow and the NSPCC are displayed in classrooms and along the corridors of the school.
- Cyber-bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyberbullying (along with all other forms of bullying) of any member of the Hollywood 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 Hollywood community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.

#### **4.4 Sexual exploitation/sexting**

- Sexting between pupils will be managed through our anti-bullying and confiscation procedures.
- All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.
- There are clear procedures in place to support anyone in the school community affected by sexting.
- All incidents of sexting reported to the school will be recorded.

#### **4.5 Radicalisation and extremism**

- Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.
- Extremism is defined by the Crown Prosecution Service as ‘The demonstration of unacceptable behaviour by using any means or medium to express views which:
  - ✓ Encourage, justify or glorify terrorist violence in furtherance of particular beliefs.
  - ✓ Seek to provoke others to terrorist acts.
  - ✓ Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
  - ✓ Foster hatred which might lead to inter-community violence in the UK.’
- Hollywood understands that there is no such thing as a “typical extremist”: those who become involved in extremist actions come from a range of backgrounds and experiences, and most

individuals, even those who hold radical views, do not become involved in violent extremist activity.

- Hollywood understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that Hollywood staff are able to recognise those vulnerabilities.
- Staff will maintain and apply a good understanding of the relevant guidance in order to prevent pupils from becoming involved in terrorism.
- Hollywood will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.
- Senior leaders will raise awareness within Hollywood about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

## **5. Communications Policy**

### **5.1 Introducing the e-safety policy to pupils**

- e-Safety rules and guidance posters will be displayed in corridors and communal spaces and discussed with pupils regularly. An e-safety display will be kept up to date in one corridor.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A program of training in e-Safety will be developed by the computing coordinator, PSHE coordinator and safeguarding lead.
- Safety training will be embedded within the computing and PSHE scheme of work in line with National Curriculum expectations.

### **5.2 Staff and the e-Safety policy**

- All staff will be given the Hollywood e-Safety Policy and have its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

### **5.3 Enlisting parents' and carers' support**

- Parents' and carers' attention will be drawn to the Hollywood e-Safety Policy in an e-safety leaflet, newsletters, the Hollywood brochure and on the Hollywood Web site.
- Hollywood will maintain a list of e-safety resources for parents/carers.
- Hollywood will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

### **5.4 Advice for parents**

- Use internet filtering software such as CyberSentinel, walled gardens and child friendly search engines. Browser controls often offer differing degrees of security for each family member.
- Check out what child protection services your Internet Service Provider (ISP) offers.
- Ensure children are using internet compatible devices in communal areas of the house.
- Tell your children not to give out any personal details. If they want to subscribe to a service (after gaining your permission) make up a family name.
- Make sure your children only use moderated chat rooms, and ask them to introduce you to their online friends.
- Encourage your children to tell you if they feel upset or threatened by what they see online.
- Write a family 'acceptable use policy' for working on the computer.
- Surf together, and be a part of their online life.

## E-Safety activities and issues

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites.	<p>Parental consent should be sought.</p> <p>Pupils should be supervised.</p> <p>Pupils should be directed to specific, approved on-line materials.</p>
Using search engines to access information from a range of websites.	<p>Filtering must be active and checked frequently.</p> <p>Parental consent should be sought.</p> <p>Pupils should be supervised.</p> <p>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.</p>
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	<p>Pupils should only use approved e-mail accounts or blogs.</p> <p>Pupils should never give out personal information.</p>
Publishing pupils' work on <b>Hollywood</b> and other websites.	<p>Pupil and parental consent should be sought prior to publication.</p> <p>Pupils' full names and other personal information should be omitted.</p> <p>Pupils work should only be published on moderated sites and by the <b>Hollywood</b> administrator.</p>
Publishing images including photographs of pupils.	<p>Parental consent for publication of photographs should be sought.</p> <p>Photographs should not enable individual pupils to be identified.</p> <p>File names should not refer to the pupil by name.</p> <p>Staff must ensure that published images do not breach copyright laws.</p>
Communicating ideas within chat rooms or online forums.	<p>Only chat rooms dedicated to educational use and that are moderated should be used.</p> <p>Access to other social networking sites should be blocked.</p> <p>Pupils should never give out personal information.</p>

<p>Audio and video conferencing to gather information and share pupils work.</p>	<p>Pupils should be supervised.</p> <p>&lt;&lt;Trust/School/Academy&gt;&gt;s should only use applications that are managed by Local Authorities and approved Educational Suppliers.</p>
<p>Social Networking</p>	<p>Staff should set their profiles to private and ensure they do not accept friend requests from pupils or parents.</p> <p>Social networking sites should be blocked on the Hollywood network.</p> <p>Pupils should be educated in the dangers involved in 'friending' or talking to people they do not know online.</p>

## Useful resources for teachers and parents

BBC Stay Safe

[www.bbc.co.uk/cbbc/help/safesurfing/](http://www.bbc.co.uk/cbbc/help/safesurfing/)

Becta

<http://schools.becta.org.uk/index.php?section=is>

Chat Danger

[www.chatdanger.com/](http://www.chatdanger.com/)

Child Exploitation and Online Protection Centre

[www.ceop.gov.uk/](http://www.ceop.gov.uk/)

Childnet

[www.childnet-int.org/](http://www.childnet-int.org/)

Cyber Café

[http://thinkuknow.co.uk/8\\_10/cybercafe/cafe/base.aspx](http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx)

Digizen

[www.digizen.org/](http://www.digizen.org/)

Kent e-Safety Policy and Guidance, Posters etc

[www.clusterweb.org.uk/kcn/e-safety\\_home.cfm](http://www.clusterweb.org.uk/kcn/e-safety_home.cfm)

Kidsmart

[www.kidsmart.org.uk/](http://www.kidsmart.org.uk/)

Kent Police – e-Safety

[www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html](http://www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html)

Think U Know

[www.thinkuknow.co.uk/](http://www.thinkuknow.co.uk/)

Safer Children in the Digital World

[www.dfes.gov.uk/byronreview/](http://www.dfes.gov.uk/byronreview/)

Care for the family

[www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf](http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf)

Childnet International "Know It All" CD

<http://publications.teachernet.gov.uk>

Family Online Safe Institute

[www.fosi.org](http://www.fosi.org)

Internet Watch Foundation

[www.iwf.org.uk](http://www.iwf.org.uk)

Kent leaflet for parents: Children, ICT & e-Safety

[www.kented.org.uk/ngfl/ict/safety.htm](http://www.kented.org.uk/ngfl/ict/safety.htm)

Parents Centre

[www.parentscentre.gov.uk](http://www.parentscentre.gov.uk)

Internet Safety Zone

[www.internetsafetyzone.com](http://www.internetsafetyzone.com)

Vodafone digital parenting

<http://www.vodafone.com/content/parents.html><http://www.vodafone.com/content/parents.html>

NSPCC - Share Aware

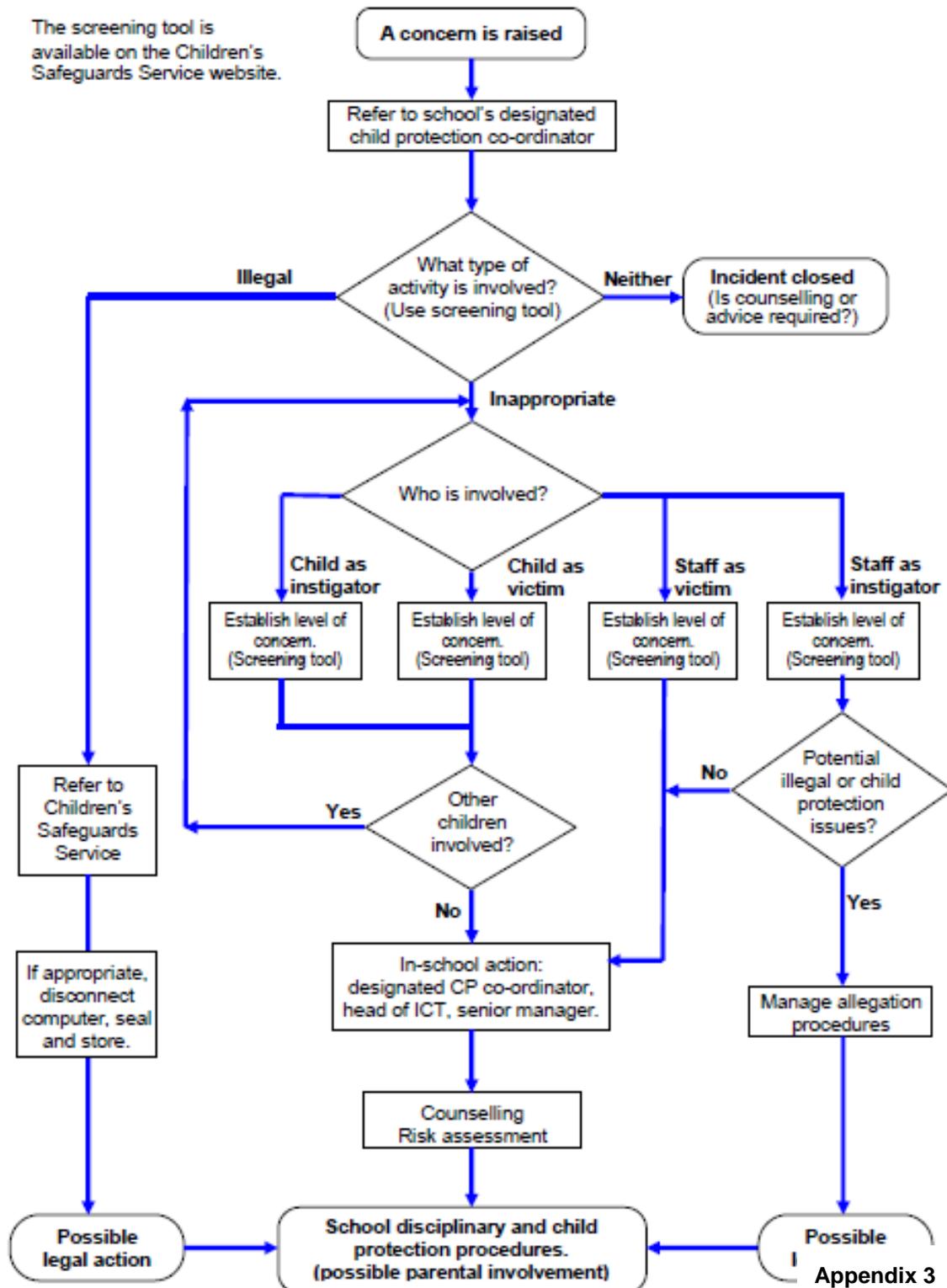
<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware>

Parent Zone

<http://www.theparentzone.co.uk/school>

## Response to an Incident of Concern

The screening tool is available on the Children's Safeguards Service website.



### Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in <<Trust/School/Academy>>. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this policy confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with <<Headteacher/Principal/Executive Headteacher>>.

- I will only use the <<Trust/School/Academy>>'s email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the <<Headteacher/Principal/Executive Headteacher>> or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the Hollywood or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other Hollywood related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of Hollywood or accessed remotely when authorised by the <<Headteacher/Principal/Executive Headteacher>> or Governing Body and with appropriate levels of security in place.
- I will not install any hardware or software on Hollywood equipment without the permission of <<Headteacher/Principal/Executive Headteacher>>
- I will report any accidental access to inappropriate materials immediately to my line manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the Hollywood network without the permission of the parent/ carer, member of staff or <<Headteacher/Principal/Executive Headteacher>> in line with data security policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the <<Headteacher/Principal/Executive Headteacher>>.

- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in Hollywood and outside <<Trust/School/Academy>>, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will support and promote the <<Trust/School/Academy>>'s e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

### User Signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the <<Trust/School/Academy>>.

Signature \_\_\_\_\_

Date \_\_\_\_\_

Full Name \_\_\_\_\_ (Printed)

**Acceptable Use Agreement: Pupils**

**Class** \_\_\_\_\_

**Year** \_\_\_\_\_

**Pupil Acceptable Use Agreement**

- I will only use ICT in Hollywood for Hollywood purposes.
- I will only use my own Hollywood email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords for the Learning Platform, Hollywood network or for other learning websites.
- I will only open/delete my own files.
- I will make sure that all ICT related contact with other children and adults is appropriate and polite.
- I will not deliberately look for, save or send anything that could offend others.
- If I accidentally find anything inappropriate on the internet I will tell my teacher immediately.
- I will not give out my personal details such as my name, phone number, home address or school address.
- I will be responsible for my behaviour when using ICT in Hollywood or at home because I know that these rules are to keep me safe.
- I will not arrange to meet someone unless this is part of a Hollywood project approved by my teacher and a responsible adult comes with me.
- I know that my use of ICT can be checked and that my parent or carer contacted if a member of Hollywood staff is concerned about my safety.
- I will not bring a mobile phone or other personal ICT device into school

Signature Pupil \_\_\_\_\_

Signature Parent \_\_\_\_\_

Date \_\_\_\_\_

## Rules for EYFS and Key Stage 1



# Think then Click



**These rules help us to stay safe on the Internet**

e-Safety Rules for EYFS and Key Stage 1

- ✓ We only use the internet when an adult is with us.
- ✓ We can click on the buttons or links when we know what they do or where they take us.
- ✓ We can use the internet to search for things when an adult is with us.
- ✓ We always stop and ask for help if we get lost on the internet.
- ✓ We can send and open e-mails with a grown-up.
- ✓ We can write polite and friendly e-mails to people we know.
- ✓ We never share our names or addresses on the internet.
- ✓ We know that friends are people we know in the real world not people we meet online.



## Rules for Key Stage 2



# Think then Click



**These rules help us to stay safe on the Internet**

## e-Safety Rules for Key Stage 2

- ✓ We ask permission before using the internet.
- ✓ We only look at websites an adult has given us permission to use.
- ✓ We always tell an adult if we have seen, heard or read anything on the internet that has made us feel threatened, uncomfortable or worried.
- ✓ We immediately close a web page if we are unsure.
- ✓ We only send polite and friendly e-mails to people we know or that an adult has approved.
- ✓ We never give out personal information or passwords.
- ✓ We never arrange to meet anyone we don't know.
- ✓ We do not open e-mails sent by anyone we don't know.
- ✓ We do not use internet chat rooms.
- ✓ We know that friends are people we know in the real world not people we meet online.



