HOLDEN CLOUGH PRIMARY SCHOOL

E-Safety and Acceptable Use Policy

November 2019

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Holden Clough Community Primary School is committed to providing quality teaching for all learners. Children are at the heart of all we do. We believe that all children and adults should enjoy learning and be actively engaged in it. Every child can do amazing things and it's our job at Holden Clough to make this potential a reality.

Introduction

The resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies and existing filtering/ security systems. Use of the Internet, by its nature, will provide access to information, which has sometimes not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these to sites unfamiliar to the teacher.
There is, therefore, the possibility that a pupil may access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet.
- Describe how these fit into the wider context of our other policies, specifically our Behaviour, ICT & Computing, PSHCE and Anti-Bullying policies.
- Demonstrate the methods used to protect the children from sites containing unsuitable material.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

At Holden Clough, we feel that the best recipe for success lies in a combination of site-filtering, supervision and by fostering a responsible attitude in our pupils in partnership with their parents/guardians.

Parents will be sent an explanatory letter and the rules, which form our Acceptable Use Agreement for pupils (attached to the end of this document) at the point they enter our school community; this will then be valid for their entire time at our school. We will also aim to disseminate any relevant published materials to parents and advise them of any changes to our policies or procedures.

E-safety forms an integral part of the children's SMSC development and contributes to these vital areas of learning.

Teaching and Learning

Why is Internet use important?

We use the internet for a number of reasons:

- Internet use is part of the statutory curriculum and 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 personal safety and security whilst online.
- 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.

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with Local Authority and the DfE;
- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet access is 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. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
- 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 taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

- The quality of information received via radio, newspaper and telephone is variable and information received via the Internet, email or text message requires even better information handling and digital literacy skills.
- In particular, it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. Pupils should be made aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject.

Managing Information Systems

How will information systems security be maintained?

- Virus protection will be updated regularly.
- Staff will only use school email addresses to communicate online.
- Portable media may not be used without specific permission followed by a virus check.

- Software should only be installed on school devices with the permission of the ICT Technician.

How will email be managed?

- Whole class or teacher email addresses will be used at Holden Clough for communication outside of school.
- Staff may only use approved email accounts for school-related emails and posts.
- Pupils will not have school email addresses and are not allowed to access personal email accounts at school. If the focus of a lesson is to use email, email simulations can be used or a class email address can be used. This will be monitored by the class teacher.
- Pupils must immediately tell a teacher if they receive offensive communications when using any message software.
- Pupils must not reveal personal details of themselves or others in any communication, or arrange to meet anyone.
- The forwarding of chain messages is not permitted.
- Staff should not communicate with pupils via email.

How will published content be managed?

- We use class blogs to celebrate pupils work, promote the school and publish resources for projects.
- Publication of information should be considered from a personal and school security viewpoint.
- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Head teacher has overall editorial responsibility and should ensure that content is accurate and appropriate and editorial guidance will help reflect the school's requirements for accuracy and good presentation.
- The website will comply with current guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

- Still and moving images and sounds add liveliness and interest to a website or blog, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.
- Although common in newspapers, the publishing of pupils' full names with their images is not acceptable.
- Images of a pupil will be published unless parents request otherwise – this can be done when the child joins our school on a consent form.
- Pupils should be taught the reasons for caution in publishing personal information and images online.

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

- Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.
- Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.
- Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- Staff need to be aware of the importance of considering the material they post on personal accounts, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
- Teachers should not make reference to their working lives on any social media.
- The school will control access to social media and social networking sites on school hardware.
- Pupils will be advised never to give out personal details of any kind, which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph, which could identify the student or his/her location.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

How will filtering be managed?

- The school will work with Network Connect to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Technician, ICT co-ordinator or a senior member of staff.
- The school’s broadband access includes filtering appropriate to the age and maturity of pupils. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that staff believe is illegal must be reported to the Head teacher, who will inform the appropriate agencies.
- We keep up to date with new technologies, including those relating to mobile phones, tablets and other handheld devices, and develop appropriate new strategies, when required.
- Personal phones should not be used to contact pupils or families. In rare circumstances, staff may have to use a personal phone to contact a parent but should consider blocking their number before they do.
- Emerging technologies will be examined for educational benefit and the Head teacher, in consultation with staff, will give permission for appropriate use.
- Mobile phones will not be used during lessons or formal school time.
- Using school hardware (e.g.iPads) to send abusive or inappropriate text, picture or video messages is forbidden by all staff and pupils.
- Pupils are not allowed to bring mobile phones into school. If a parent wishes their child to bring a mobile phone to school, it must be placed in the school office at the start of the day and collected at the end of the day.

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 (“the Act”) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly.

It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

This section is a reminder that all data from which people can be identified is protected. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

How will Internet access be authorised?

- We allocate Internet access for staff and pupils on the basis of educational need. It should be clear who has Internet access and who has not.
- Usage is supervised. Normally all pupils will be granted Internet access.
- Parental permission is required for Internet access in all cases as new pupils Holden Clough.
- All staff must read and sign the Acceptable Use Policy for Staff before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.

How will risks be assessed?

- Milton St. John's 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 will not accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly and after every breech of this policy.

How will e–Safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the school's complaints procedure.
- Any complaint about staff misuse must be referred to the Head teacher. If the complaint is about the Head teacher, this should be reported to the Chair of Governors.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.
- Parents and pupils will work in partnership with staff to resolve issues.

- Discussions will be held with the local Police if anything potentially illegal arises.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

How is the Internet used across the community?

- We recognise that children can access the internet outside of school and offer support and advice to parents on internet safety though information sent home and regular e-safety workshops.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Pupils will be taught about E-safety issues every year as part of their class curriculum. It will also be covered if and when issues arise and as the Internet is used, where appropriate.
- We also hold an E-safety evening at least once every two years. This is aimed at the parents/carers of children from Year 1 to Year 6. The evening is a workshop to teach parents/carers about the dangers their children may come across online and offers some practical advice.

How will Cyberbullying be managed?

- Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.
- It is essential that pupils, Milton St. John's staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.
- Promoting a culture of confident users will support innovation and safety.
- Childnet has produced resources and guidance that will be used to give practical advice and guidance on cyberbullying:
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded.

There are clear procedures in place to investigate incidents or allegations of bullying:

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include: The perpetrator will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers will be informed and the Police will be contacted if a criminal offence is suspected.

Other E-safety Issues

- **Sexting** – older children will be sensitively informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the world wide web.
- **Pornography –** many children will come across some type of pornographic content when searching the Internet. Children are taught about what to do if they come across this type of material and who to speak to.
- **Trolling** – children will be taught about being kind and respectful of others online. They will know about the effect their actions can have on others and their own future employment opportunities. They will also be taught what to do if they are a victim of online abuse.

- **Fraping** – the children will be made aware that it is inappropriate to access someone else's online accounts and how posting as someone else is not acceptable.
- **Grooming** – older children will be sensitively taught about the dangers of Internet predators and the process of grooming.
- **Radicalisation** – older children will be informed about how the Internet can be used to insight people to do radical and harmful things. They will be warned about propaganda and the untruthful things that can be viewed online.
- **Cyber self-harm** – older children will be informed about not deliberately harming themselves by what they post online. They will be taught about talking about problems with real people, especially trusted adults.

We will try to keep up-to-date with new terminology and react to those as appropriate.

Communication Policy

How will the policy be introduced to pupils?

- At Milton St John's we teach about e–safety as a separate ICT & Computing unit and also as part of every subject whenever pupils are using the Internet.
- All users are informed that network and Internet use will be monitored.
- Pupil instruction in responsible and safe use should precede Internet access every time they go online.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

We will use many different resources, including the following e–Safety programmes:

Think U Know: www.thinkuknow.co.uk
Childnet: www.childnet.com
Kidsmart: www.kidsmart.org.uk
Safe Social Networking: www.safesocialnetworking.com

How will the policy be discussed with staff?

- The e–safety policy will be formally provided to and discussed with all members of staff and published on the school website.
- To protect all staff and pupils, the school will implement Acceptable Use Policies. Staff should be aware that Internet traffic can be monitored and traced to the individual user; discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided, both internally and externally, as appropriate.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e–safety policy in newsletters, the school brochure, letters and on the school website.
- A partnership approach with parents will be encouraged.
- Parents will be requested to sign an e–safety/internet agreement as part of the school's on entry procedures. Information and guidance for parents on e–safety will be made available to parents in a variety of formats.

Policy Management

This policy is linked to the following mandatory school policies: Child Protection, Whistle Blowing, Health and Safety, Anti-Bullying, Home School Agreements, ICT & Computing and PSHE**.**

Who will review the policy?

The e–Safety Policy and its implementation will be reviewed annually.

Acceptable Use Policy (AUP)

Staff Agreement

This document covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, the school website, blogs, all software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system for any school business (your school email address).
- I will not communicate with pupils or parents/carers online, except via the school website, class dojo or blog.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the head teacher.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti- virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils and will not store images at home. Images of children will only be stored on the school server unless stored on the Ipad and uploaded for the blogs.
- I will ensure that laptops will be closed and any recording equipment linked to computers turned off when get children change for PE/ or any other activities. Ipads or any other handheld device will not be used during these times.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are private and are not in conflict with my professional role.
- I will not communicate with pupils/parents (past or present) via social media. (The exception to this is when staff communicate via class dojo to parents of present pupils for that academic year.)
- I agree and accept that any computer, laptop or iPad loaned to me by the school, is provided solely to support my professional responsibilities.
- I will ensure any confidential data that I wish to transport from one location to another is protected by a password/passcode and/or encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be

kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will embed the school's e-safety curriculum into my teaching.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to the school management on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I wish to have an email account; be connected to the Internet and to use the school's ICT resources and systems.

Signature ....

Full Name ....

Date ....

Job title ....

Internet Agreement – E-Safety Rules
(Acceptable Use Policy – Pupils)

All pupils and their parents/carers are asked to read and sign an agreement covering the expectations we have of pupils using the Internet in school.
This is to be read through with your parent/carer(s) and then signed. You will be allowed Internet Access after this is returned to school.

At Holden Clough Community Primary School, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- Pupils using the World Wide Web (Internet) are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Pupils are expected not to use any rude language in their communications and contact only people they know or those the teacher has approved.
- Pupils must ask permission before accessing the Internet.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on disc or USB drive should be brought in from home for use in school, unless permission has been given by the class teacher.
- Any USB drive brought in will be virus scanned by the class teacher before use.
- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made.
- Pupils choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

I have read through this agreement with my child and agree to these e-safety restrictions.

Signed: ____ (Parent/Carer)

Name of child: _______________________________________

Holden Clough Community Primary School

E-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the E-Safety Rules have been understood and agreed.

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images/videos that include my son/daughter may be published on the school website, including the school blogs, subject to the school rule that photographs will not be accompanied by pupil's full names.

I also understand that any photographs that either myself or my son/daughter take of a class assembly or during a school trip/event are for our personal use and should not be used for any other purpose.

Parent's Consent for Internet Access

I have read and understood the school E-Safety rules and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

I understand that if my child breaks any of the E-Safety rules, sanctions will be applied, which could include a ban from using the school computers.

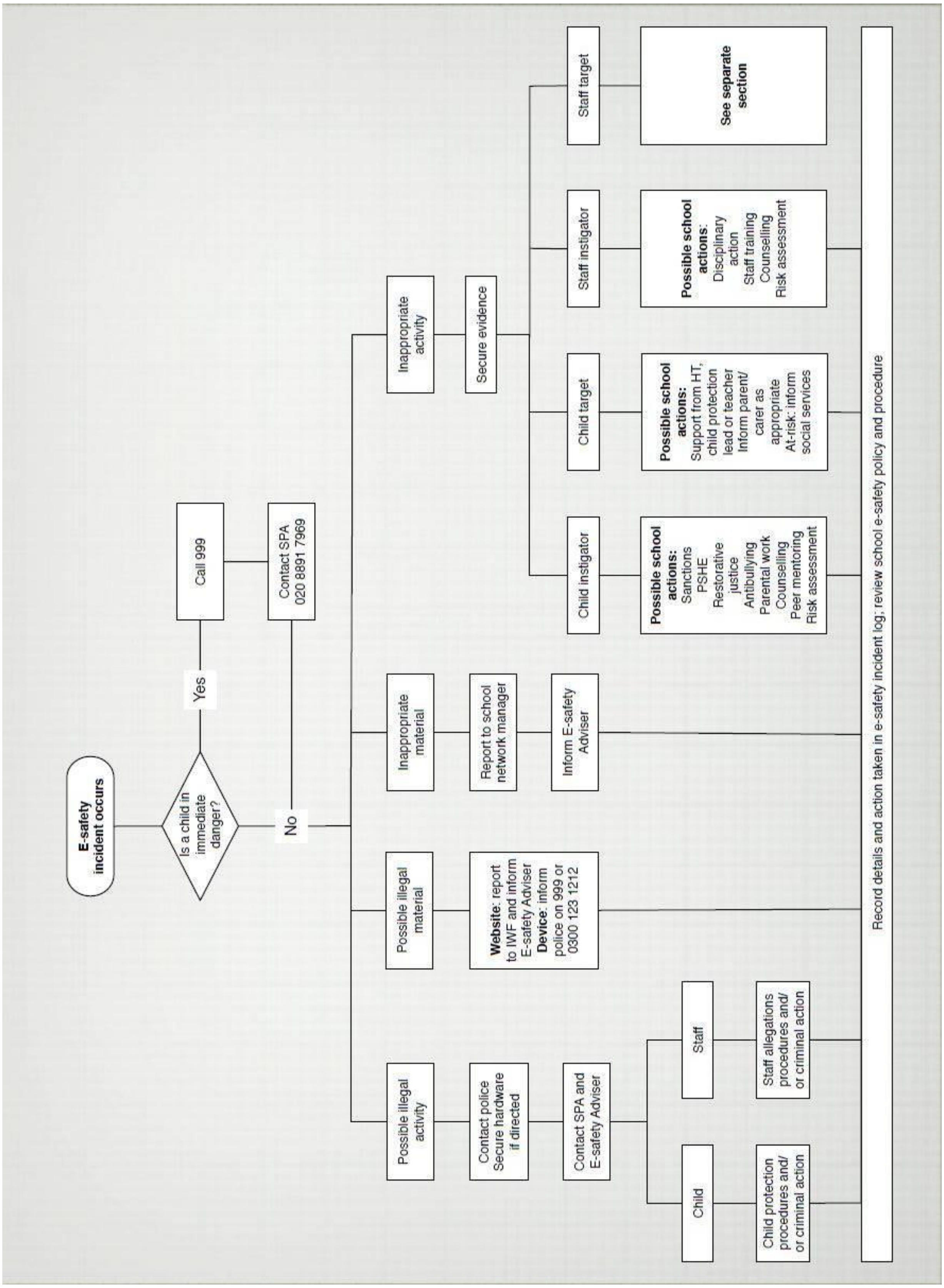
Signed:

Date:

Child's name:

Please complete, sign and return to the school

Appendix A:


E-safety incident occurs
Is a child in immediate danger?
Yes
Call 999
Contact SPA 020 8891 7969
No
Possible illegal activity
Contact police Secure hardware if directed
Contact SPA and E-safety Adviser
Child
Child protection procedures and/ or criminal action
Staff
Staff allegations procedures and/ or criminal action
Possible illegal material
Website: report to IWF and inform E-safety Adviser Device: inform police on 999 or 0300 123 1212
Inappropriate material
Report to school network manager
Inform E-safety Adviser
Inappropriate activity
Secure evidence
Child instigator
Possible school actions: Sanctions PSHE Restorative justice Antibullying Parental work Counselling Peer mentoring Risk assessment
Child target
Possible school actions: Support from HT, child protection lead or teacher Inform parent/ carer as appropriate At-risk: inform social services
Staff instigator
Possible school actions: Disciplinary action Staff training Counselling Risk assessment
Staff target
See separate section
Record details and action taken in e-safety incident log; review school e-safety policy and procedure