Pot Kiln School

E-Safety Policy

Review Date: Autumn 2018
Next Review Date: *Summer 2019*

Date of document review (as per cover)	Document changes

Signed: Date:

Designation:

Approved: Date:

Designation:

Section

1. Statement of Intent

Introduction

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of school/education setting or other establishments to ensure that children and young people are protected from potential harm both within and beyond the School environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

Aims

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-safety' and digital wisdom are used to encompass the safe use of all technologies in order to protect children, young people and adults and reduce potential and known risks.

- To emphasise the need to educate staff, children and young people about the positives and negatives of using new technologies both within and outside School.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.
- To ensure that adults are aware of their responsibilities for Data Protection and disposal of redundant electrical and electronic equipment.

2. Responsibilities of the Governors

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of e-Safety (Digital wisdom) as part of the wider remit of safeguarding across the School with further responsibilities as follows:

- At the Full Governor meetings, all Governors are to be made aware of e-Safety developments from the Curriculum meetings.
- The Governors **MUST** ensure e-safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.
- *The Head teacher, along with the Governors will adopt the standard disclaimer on all e-mails stating that the views expressed are not necessarily those of the school/education setting or other establishment, the LA or organisation.*
- It is the responsibility of the Safeguarding Governor to challenge the school about having an Acceptable Use Agreement (AUA) (see Appendix 2&3) and policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT. This should include ensuring that the School has adequate;
    - Firewalls.
    - Anti-virus and anti-spyware software.
    - Filters.
    - Using an accredited ISP (internet Service Provider).
    - Awareness of wireless technology issues.
    - A clear policy on using personal devices.
- The Governors must ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, (see the Managing Allegations Procedure on Suffolk Local Safeguarding Children's Board website) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers. http://suffolksafeguardingchildrenboard.onesuffolk.net/assets/files/AllegationsmadeAgainstStaffEducationSettings.pdf

3. Responsibility of the Head Teacher

- The Head Teacher should inform the Governors about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure that the Governors know how this relates to safeguarding.
- The Head Teacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the School development plan. The Acceptable Use Agreement should be reviewed and issued annually.
- The Head Teacher is responsible that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform .
- The Head Teacher will designate an e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements.
- The Head Teacher will provide time on request for the e-safety lead to remain up to date with new curriculum and technological developments.

- There will be transparent monitoring of the Internet and online technologies. The school will be part of the Suffolk Proxy server to ensure safe usage within school

- Ensure that unsolicited e-mails to a member of staff from other sources is minimised – *by ensuring all staff use school e-mail address rather than personal. (*Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received) http://suffolksafeguardingchildrenboard.onesuffolk.net/assets/files/AllegationsmadeAgainstStaffEducationSettings.pdf

- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified (appendix 1) in an incident report log (appendix 5)

- Keep a record of all the signed Acceptable Use Agreement forms.

4. Responsibilities of the e-safety lead

- Report issues and update the Head Teacher on a regular basis.
- Ensure e-Safety is addressed, in conjunction with the IT technician, in order to establish a safer computing learning environment, through the use of
    - Firewalls.
    - Anti-virus and anti-spyware software.
    - Filters.
    - Using an accredited ISP (internet Service Provider).
    - Awareness of wireless technology issues.
    - A clear policy on using personal devices (see Acceptable Use policy
- Time and resources will be utilized at the request, to ensure the e-Safety Lead is aware of new curriculum and technological developments.
- Staff to be trained, implement and update policies, as appropriate.
- Ensure that filtering, up to date anti-virus and anti-spy software is set to the correct level for staff, children and young people on stand-alone PC, staff/children laptops and the learning platform in conjunction with the IT technician. This should be reviewed termly and as required.
- The e-Safety Lead and a senior member of staff will monitor the use of online technologies by children and young people and staff, on an ongoing basis.
- The e-Safety lead will provide an information leaflet for parents to encourage them to be aware of how to stay safe on line and set privacy settings at home.

5. Responsibilities of all adults.

It is the responsibility of all adults within the school to:

- Appreciate the importance of e-Safety within School and to recognise that they have a general duty of care to ensure the safety of their pupils and staff.
- All staff are responsible for ensuring that they are aware of who takes the role of the e-Safety lead within the school environment.
- All staff are responsible for ensuring safe use of IT in line with the social networking policy, Acceptable Use Policy and the e-Safety policy.
- Ensure that they know who the Senior Designated Person for Safeguarding is within school so that any misuse or incident involving a child can be reported promptly. (Head teacher and Deputy Head teacher)
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures should be followed immediately.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the Suffolk County Council accident/incident reporting procedure
- All adults should be aware of the filtering levels and why they are there to protect children and young people.
- Alert the e-Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Report accidental access to inappropriate materials to the e-Safety Lead in order that inappropriate sites are added to the restricted list..
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Teachers should monitor the use of the Virtual Learning Platform and Internet during lessons and also monitor the use of e-mails from school and at home, on a regular basis.
- Ensure that the tone of e-mails is in keeping with the ethos of the school. Blanket e-mails are discouraged. Report overuse of blanket e-mails or inappropriate tones to the Head teacher and/or Governors.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Ensure children and young people know what to do in the event of an incident and adopt the ‘never blame the child for accidentally accessing inappropriate materials’ culture,
- Sign an Acceptable Use Agreement to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the School environment, as outlined in appendices 2&3.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. http://www.suffolk.gov.uk/assets/suffolk.gov.uk/Your%20Council/FOI/2010-01-11%20DataProtectionPolicy.pdf .
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/education setting or other establishment's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
- Have access to the network, so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

In the Event of Inappropriate Use

- If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted (appendix 1) http://suffolksafeguardingchildrenboard.onesuffolk.net/assets/files/AllegationsmadeAgainstStaffEducationSettings.pdf

6. Responsibilities of all students and parents/carers.

Children and young people should:

- Be involved in the review of Acceptable Use Agreement through the school council in line with this policy being reviewed and updated.
- Each child or young person should receive a copy of the Acceptable Use Agreement on an annual basis and on first-time entry to the school which needs to be read with the parent/carer, signed and returned to school, confirming both an understanding and acceptance of the agreement.

(The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child,)

- It is expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted. Any potential issues that parents/carers feel should be addressed, will be considered as appropriate.
- The agreement should be on display within the classrooms and computer suite, where this may be applicable.
- Children and young people should be taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).
- Students and parents will be made aware of this policy and the individual responsibilities of acceptable use (see appendix 3)
- Parents to feel informed and know where to go for advice. The school will do this by holding an e-safety **Parent/Carer Information Evening** once per annum.

Part of this evening will provide parents with information on how the school protects children and young people whilst using the learning platform facilities, such as the Internet and E-mail. It will also be an opportunity to explore how the school is teaching children and young people to be safe and responsible Internet users and how this can be extended to use beyond the school environment.

In the Event of Inappropriate Use

- Should a child or young person be found to misuse the online facilities whilst at school the following consequences should occur:
  - Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person’s use for a particular lesson or activity.

- Further misuse of the agreement may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.

- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

- Any misuse of the agreement will result in appropriate sanctions which will be in line with the school behaviour policy.

- In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, e.g. use 'Hector Protector', for example, (dependent on age) so that an adult can take the appropriate action.

- Children should be made aware of **Hector Protector,** which shuts down the computer screen should they feel uncomfortable about the content they have accessed.

- Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

- Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites as this may have legal implications.

7. The Curriculum and Tools for Learning

The school should teach children and young people how to use the Internet safely and responsibly. They should also be taught, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave *Year 6*.

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

The children need to be taught how to access resources online through the use of the schools learning platform 'DP Primary' where usage and communication can be monitored by the school.

Children should be taught how to explore on-line technologies in a safe and responsible manner including how to deal with personal safety using Hector Protector and www.thinkuknow.co.uk

a. Personal safety

- Ensure information uploaded to web sites and e-mailed to other people does not include any personal information such as:
  - Full name (first name is acceptable, without a photograph).
  - Address.
  - Telephone number.
  - E-mail address.
  - School/education setting or other establishment.
  - Clubs attended and where.
  - Age or DOB.
  - Names of parents.
  - Routes to and from school/education setting or other establishment.
  - Identifying information, e.g. I am number 8 in the School Football Team.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to policy.

b. Pupils with Additional Learning Needs

The school should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-Safety awareness sessions and internet access.

c. Learning Platforms

Suffolk's learning platform provides a wealth of opportunity for adults, children and young people within and beyond the school setting to:

- Access resources via the National Education Network (NEN), which extends regionally to support school/education setting or other establishments.
- Collaborate and share work via web cams and uploading.
- Ask questions.
- Debate issues.
- Dialogue with peers.
- Dialogue with family members or carers.
- Access resources in real time.
- Access other people and cultures in real time.
- Develop an online community.

The tools available for use within the learning platform for adults and children include:

- Internet access.
- E-mail.
- Video-conferencing.
- Weblogs (online diaries).
- Wikis (online encyclopaedia or dictionary).
- Instant Messaging.
- An online personal space for adapting as a user to:
    - Upload work.
    - Access calendars and diaries.
    - Blog.

The personal space contained on a learning platform is designed to provide young users with the facility to share information and work collaboratively with others members of Suffolk's enable community. It should be noted that learning platforms provide the user with a private area where they may store information about themselves, accessible only to other platform users via an 'invite' system. Before students access and populate this area, guidance and support should be given to young people regarding the appropriate use of personal details on social networking sites (such as Facebook, twitter, club penguin, Moshi Monsters and Bebo) and how to keep themselves safe whilst online.

Children should use their login and password to access the internet via the learning platform so that the level of filtering is appropriate. Staff should be ensuring that children and young people are not bypassing the login to get to the learning platform so that they are protected to the best of the school's ability, in line with the filtering system (E2BN) and AUA.

8. Web sites

a. School Website

- The uploading of images to the School website should be subject to the same acceptable agreement as uploading to any personal online space.
- Permission must be sought from the parent/carer prior to the uploading of any images.
- The school should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

b. External Websites

- In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, schools are encouraged to report incidents to the Head Teacher and unions, using the reporting procedures for monitoring.

9. E-mail Use Advice

- The school should have E-mail addresses for children and young people to use, as a class and/or as individuals through DP Primary as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

- Staff, children and young people should use their school issued email addresses for any communication between home and school. A breach of this may be considered a misuse.

- Parents/carers are encouraged to be involved with the monitoring of emails sent, although the best approach with children is to discuss with the child about who they may be talking to and assess risks together.

- Teachers are expected to monitor their class use of emails where there are communications between home and school as required.

10. Mobile Phones and Other Emerging Technologies

- The use of mobile technologies can be used as a teaching and learning tool within the curriculum with the following areas of concern to be taken into consideration:

  - Inappropriate or bullying text messages.
  - Images or video taken of adults or peers without permission being sought.
  - 'Happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed.
  - Sexting - the sending of suggestive or sexually explicit personal images via mobile phones.
  - Wireless Internet access, which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

If a child brings a mobile device to school it should be retained by the teacher for safe keeping and reissued back to them at the end of the day thus reducing the risk of abuse with school.

c. Personal Mobile Devices (see Acceptable use Policy)

- Staff should be allowed to bring in personal mobile phones or devices for their own use at the appropriate time, but **must not use personal numbers to contact children under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras
- Staff should be aware that games consoles such as the Sony play station, Microsoft Xbox, Nintendo Wii and DSi and other such systems have Internet access which may not include filtering. **N.B.** Before use within school authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.
- The School is not responsible for any theft, loss or damage of any personal mobile device.

d. School Issued Mobile Devices

- The management of the use of these devices should be similar to those stated above, but with the following additions:

- Where the school has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, only this equipment should be used to conduct school setting or other establishment business outside of the school setting or other establishment environment.

11. Video and Photographs

The term ‘image’ refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in school there is access to:
Cameras
Flip video cameras
IPads
Laptops

- Photographic permission must be sought prior to uploading of any images onto the school network and use within school.

- Photographs must be stored in a central location on the Network and put into appropriate folders within one week and deleted from any other device within this time.

- Photograph folders will be deleted one year after the children have left the school.

- The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.

- Photographs/images used to identify children in a forum or using Instant Messaging within the learning platform should be a representative of the child rather than of the child e.g. an avatar.

- Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a School website. Photographs should only ever include the child’s first name although safeguarding guidance states either a child’s name or a photograph but not both.

- Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit.

- It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of children/young people should only be used after permission has been given by a parent/carer.

12. Video-Conferencing and Webcams

- Flash meeting is the main video conferencing service provided by E2BN which allows staff to preset a secure ‘conference room’ which remains under their control throughout the session. The use of webcams to video-conference will be via E2BN which is a filtered service. Publicly accessible webcams are not used in school.

- Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

- Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

13. Managing Social Networking and Other Web 2.0 Technologies (see also Social Networking Policy)

Social networking sites have emerged in recent years. The service offers users both a public and private space through which they can engage with other online users. This technology opens a gateway to online communication with young people. There are a number of risks associated which must be addressed.

In response to this issue the following measures should be put in place:

- The school should control access to social networking sites through existing filtering systems.
- Students are advised against giving out personal details or information, which could identify them or their location
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Facebook now hold rights to any picture or post placed onto its website even when deleted. Advice is also given regarding background images in photos, which could reveal personal details
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to ‘Friends only’ for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The School should be aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to the School allowing for the procedures, as set out in the anti-bullying policy, to be followed.

- The school will provide an information leaflet for parents to encourage them to be aware of how to stay safe on line and set privacy settings at home.

Social Networking Advice for Staff
(see Social Networking policy for further details)

Social networking outside of work hours, on non-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. (see social networking policy for advice.

Links to Other Policies - Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, social networking sites, e-mail or blogs.

Managing Allegations against Adults Who Work With Children and Young People

Please refer to the Managing Allegation Procedure, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegations of misuse or misconduct being made by any member of staff or child about a member of staff.

14. Health and Safety

Refer to the Health and Safety Policy and procedures of the School and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

15. Disposal of ICT and electronics /electrical equipment.

The Waste Electrical & Electronic Equipment (WEEE) directive is now law regarding redundant equipment and must be disposed of via a specialist contractor.

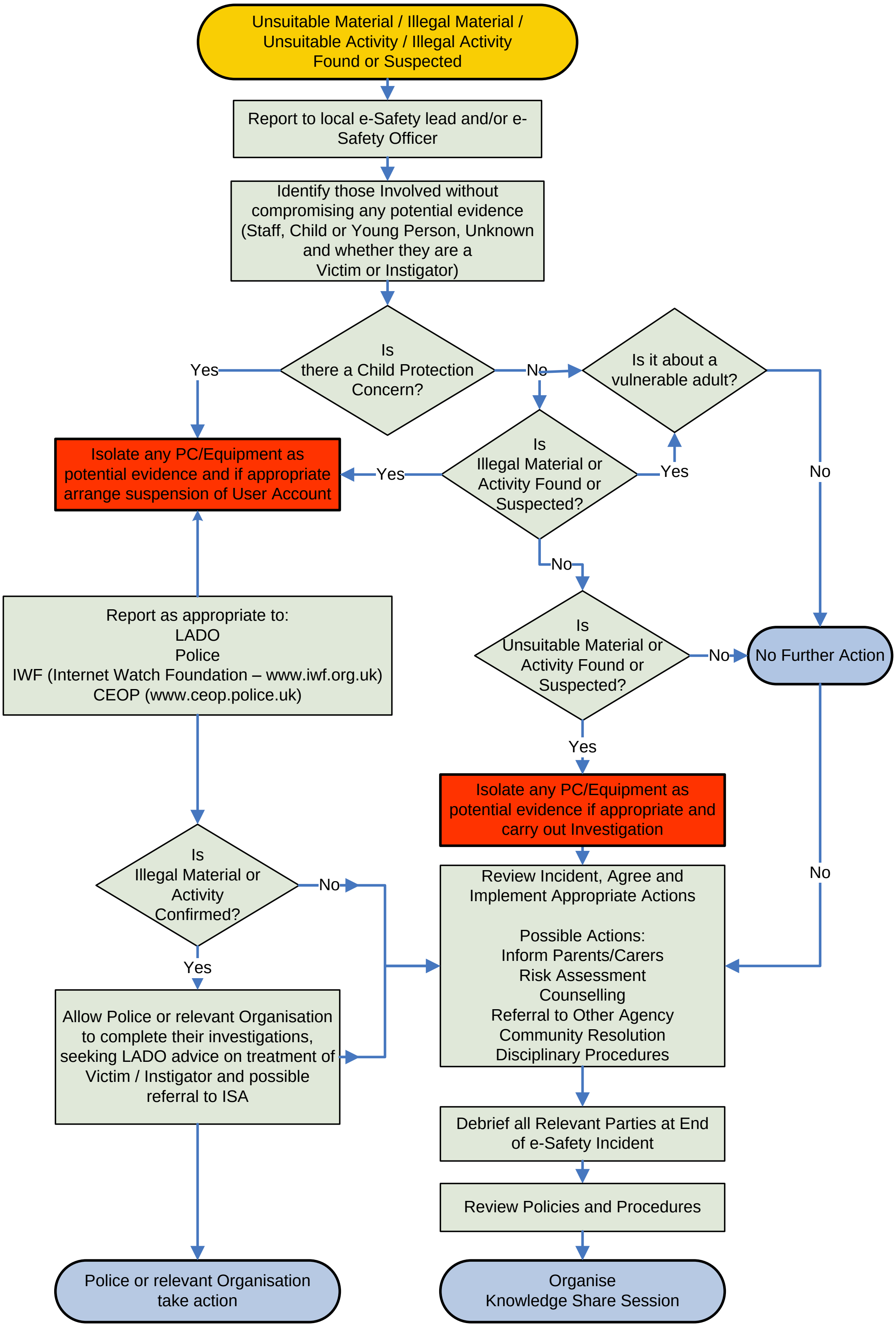
Data Protection

Schools also need to be mindfully of the Data Protection Act and that the school will be liable for any data that gets into the public domain as a result of a failure to fully wipe IT equipment hard drives. The school should ensure if they are planning to sell on any redundant equipment that they use specialist contractors to wipe the hard drive and a certificate proving the work was completed should be obtained.

Schools also need to ensure that all software is removed from the devices as there are licensing implications where schools receive substantial discounts that cannot be sold on for personal use.

See Finance policy for details of disposal/ redundant ICT and electronic/electrical equipment and specialist contractors to be used.

Fig 1: e-Safety Flow Chart



Unsuitable Material / Illegal Material / Unsuitable Activity / Illegal Activity Found or Suspected
Report to local e-Safety lead and/or e-Safety Officer
Identify those Involved without compromising any potential evidence (Staff, Child or Young Person, Unknown and whether they are a Victim or Instigator)
Is there a Child Protection Concern?
Yes
No
Is it about a vulnerable adult?
Isolate any PC/Equipment as potential evidence and if appropriate arrange suspension of User Account
Yes
Is Illegal Material or Activity Found or Suspected?
Yes
No
No
Report as appropriate to: LADO Police IWF (Internet Watch Foundation – www.iwf.org.uk) CEOP (www.ceop.police.uk)
Is Unsuitable Material or Activity Found or Suspected?
No
No Further Action
Yes
Isolate any PC/Equipment as potential evidence if appropriate and carry out Investigation
Is Illegal Material or Activity Confirmed?
No
Review Incident, Agree and Implement Appropriate Actions
Possible Actions: Inform Parents/Carers Risk Assessment Counselling Referral to Other Agency Community Resolution Disciplinary Procedures
No
Yes
Allow Police or relevant Organisation to complete their investigations, seeking LADO advice on treatment of Victim / Instigator and possible referral to ISA
Debrief all Relevant Parties at End of e-Safety Incident
Review Policies and Procedures
Police or relevant Organisation take action
Organise Knowledge Share Session

APPENDIX 1

APPENDIX 2

Acceptable Use Agreement for Staff, Governors, Volunteers and Visitors.

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. You are asked to sign this Acceptable Use Agreement so that you provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect you so that you feel safeguarded from any potential allegations or inadvertent misuse.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I know the sanctions for misuse, so that I can effectively deal with any problems that may arise.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person’s safety to the Headteacher, Senior Designated Person or e-Safety Lead.
- I know who my Senior Designated Person is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use the school e-mail address and phones (if provided) and only to a child’s school e-mail address upon agreed use within the school.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Lead.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.

- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Acceptable Use Agreement to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree with this Agreement as I know that by following it I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed……………………………………………….Date…………………….

Name (printed)………………………………………………….

School……………………………………………

APPENDIX 3

Acceptable Use Policy for Young People

My e-Safety Agreement

This is my agreement for using the internet safely and responsibly.

- I will use the internet to help me learn.
- I will learn how to use the internet safely and responsibly.
- I will only send email messages that are polite and friendly.
- I will only email, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video conferencing.
- I agree never to give out passwords or personal information like my full name, address or phone numbers.
- I agree never to post photographs or video clips without permission or that I will not include my full name with photographs.
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to a trusted adult.
- If I see anything on the internet that makes me feel uncomfortable, I know what to do.
- If I receive a message sent by someone I don't know, I know what to do.
- I know I should follow these guidelines as part of the agreement with my parent/carer.
- I agree to look after myself and others by using my internet in a safe and responsible way.

APPENDIX 4

Pot Kiln School

Dear Parent/ Carer

Information Computer Technology (ICT) including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E -Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact The Head Teacher.

- -✂- -

Parent/ carer signature
We have discussed this and …………………………………………….(child name) agrees to follow the e-Safety rules and to support the safe use of Information Computer Technology at Pot Kiln Primary School.

Parent/ Carer Signature ……………………….………………………

Class …………………………………. Date ………………………………

APPENDIX 5

Pot Kiln Primary School e-Safety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons