HILLSIDE SPECIAL SCHOOL

ONLINE SAFETY AND ACCEPTABLE USE OF THE INTERNET AND OTHER MODERN TECHNOLOGY POLICY

Policy reviewed: October 2017

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 to ensure that children and young people are protected from potential harm both within and beyond the school. 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 'Online Safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff, children or young people, 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.

Roles and Responsibilities of the School

Governors and Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of Online Safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Headteacher has designated an Online Safety Lead (the named person is Shelley Jackson, Deputy Headteacher) to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring Online Safety is addressed in order to establish a safe ICT learning environment. All staff are made aware of this role within the school.
- Time and resources are provided for the Online Safety Lead and staff to be trained and update policies.
- The Headteacher is responsible for promoting Online Safety across the curriculum and has an awareness of how this is being developed, linked with the School Development Plan.
- The Headteacher should inform the Governors about the progress of, or any updates to the Online Safety curriculum (via PSHE or Computing) and ensure Governors know how this relates to safeguarding.

- The Governors must ensure Online 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 school has a designated Online Safety Governor, Pauline Lucas. The Online Safety Governor ought to challenge the school about having an Online Safety and Acceptable Use Policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:

  Challenging the school about having:
    - Firewalls
    - Anti-virus and anti-spyware software
    - Filters
    - Using an accredited Internet Service Provider (ISP)
    - A clear policy on using personal devices
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, (see the Managing Allegations Procedure on Suffolk 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.

Online Safety Lead

It is the role of the designated Online Safety Lead to:

- Appreciate the importance of Online Safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Ensure that the Online Safety and Acceptable Use Policy is reviewed annually, with up-to-date information and that training is available for all staff to teach Online Safety and for parents to feel informed and know where to go for advice.
- Ensure 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 or ensure the technician is informed and carries out work as directed.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, Safeguarding and Computing Leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct Online Safety information can be taught or adhered to.
- Ensure transparent monitoring of the internet and online technologies.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to the Managing Allegations Procedure from the SSCB to ensure the correct procedures are used with incidents of misuse.
- Work alongside the Computing Lead, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.

Staff or Adults

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

- Ensure that they know who Designated Safeguarding Lead (DSL) is within school, so that any misuse or incidents can be reported which involve a child can be reported.
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher/ Designated Safeguarding Lead. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately (following the Managing Allegation Procedure SSCB).
- Be familiar with the Behaviour, Anti-Bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher/ Designated Safeguarding Lead immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the Online Safety Lead.
- Alert the Online Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- 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. Children and young people should know what to do in the event of an incident.
- Be up-to-date with Online Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Agreement to show that they agree with and accept the agreement for staff using school equipment, within and beyond the school, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a computer unlocked when logged in but not at the station.
- Follow the correct procedures for any data required to be taken from the school.
- Report accidental access to inappropriate materials to the Online Safety Lead in order that inappropriate sites are added to the restricted list or control this with the Local Control options via the broadband connection.
- 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'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.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the SCC accident/incident reporting procedure in the same way as for other non-physical assaults.
- Do not send private, sensitive or confidential information by unencrypted email if disclosure could lead to significant harm or embarrassment. Personal data should be anonymous where possible e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients.
- Staff who have been given the use of a school laptop will be expected to sign for its use on receipt. Staff may use school equipment for authorised school use only, except as allowed for in the Personal Use and Privacy section of this policy.

Children and Young People
Children and young people should:

- Be helped to use the internet in a safe and responsible manner through Computing and PSHE
- Be encouraged to gain awareness of Online Safety from the "How to use the internet safely" rules.
- Be encouraged to tell a member of staff about any inappropriate materials or contact from someone they do not know straight away.
- Only have access to the internet with appropriate level of content filtering as set by the proxy server.
- Only have access to the internet or electronic mail under the supervision of a member of staff.
- Be logged on to the school system using their 'Class' login usernames and passwords in order to ensure that all internet content is filtered.

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

Staff 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 unlocked and unattended whilst they are logged in.

All staff should receive a copy of the Online Safety and Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school, to keep under file with a signed copy returned to the member of staff.

The Online Safety and Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations.

No one may use ICT resources to transmit abusive, threatening or harassing material, chain letters, spam or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists and other public forums through which they participate from a school account.

The following content should not be created or accessed on ICT equipment at any time:

- Pornography and "top shelf" adult content
- Images of children or adults that could be considered inappropriate
- Material that gratuitously portrays images of violence, injury or death
- Material that is likely to lead to the harassment of others
- Material that promotes intolerance and discrimination on the grounds of race, sex, disability, sexual orientation, religion or age
- Material relating to criminal activity, for example buying and selling illegal drugs
- Material relating to any other unlawful activity e.g. breach of copyright
- Material that may generate security risks and encourage computer misuse

It is possible to access or be directed to unacceptable internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Online Safety Lead immediately. This may avoid problems later should monitoring systems be alerted to the content.

Personal Use and Privacy
In the course of normal operations, ICT resources are to be used for business purposes only. The school permits limited personal use of ICT facilities by authorised users subject to the following limitations:

- Personal use does not extend to accessing social networking sites from school facilities
- Personal use must be in the users' own time and must not impact upon work efficiency or costs
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided
- Personal use must not be of a commercial or profit making nature
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations

In the Event of Inappropriate Use

By a Member of Staff
If a member of staff is believed to misuse the internet in an abusive or illegal manner, a report must be made to the Headteacher / Designated Safeguarding Lead immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

By Children or Young People
Online Safety & Acceptable Use of ICT Rules for children and young people are outlined in the Appendices. These detail how they are expected to use the internet and other technologies within Hillside Special School. The rules are there for children and young people to understand what is expected of them when using the internet.

The rules should be on display within the classrooms and computer suite.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- In the event that a child or young person is found to be misusing the internet, the Headteacher should be informed so that the appropriate action can be taken.
- In the event that a child or young person accidentally accesses inappropriate materials they should report this to an adult immediately and take appropriate action to hide the screen or close the window, using 'Hector Protector' so that an adult can take the appropriate action.
- Children should be taught and encouraged to consider the implications for misusing the internet.

The Curriculum and Tools for Learning

Internet Use
School should teach children and young people how to use the internet safely and responsibly. They should also be taught, through Computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further

learning. Depending on the capabilities of the children and young people, the following concepts, skills and competencies should be taught:

- 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
- 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 SCC Primary Computing Scheme of Work can be used to teach internet and E-mail lessons. Online Safety lessons and resources can also be found at www.thinkuknow.co.uk for KS1 and KS2.

All pupils should be taught Online Safety as part of the National Curriculum for Computing, so school will need to explain how they are addressing the needs of this aspect of the curriculum, e.g. most pupils recognise the need to be safe and act responsibly when using digital communications.

The www.thinkuknow.co.uk resources for 11-16 years olds can be used, with free training provided to teachers/adults for the delivery of these lessons. Further training advice can be sought from Suffolk online safety Lead or by going to the website.

These skills and competencies are taught within the curriculum as appropriate, so that children and young people have the security to explore how online technologies can be used effectively, but in a safe and responsible manner.

Personal safety – ensuring 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
- Clubs attended and where
- Age or DOB
- Names of parents
- Routes to and from school
- Identifying information, e.g. I am number 8 in the school football team.

Images of children and young people must not be uploaded to the internet.

Learning Platforms

Hillside's use of Suffolk's learning platform is at an early stage of development and therefore the following section is for information only at present. Should the school make use of the learning platform in the future, this statement will be amended accordingly.

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

- Access resources via the National Education Network (NEN), which extends regionally to support school
- 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, children and young people 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 enabled 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 and Bebo) and how to keep themselves safe whilst online.

Children and young people should use their login and password to access the learning platform so that the level of filtering is appropriate.

Staff or adults need to ensure they consider the risks and consequences of anything they or their children and young people may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and the school.

School Website

The uploading of images of pupils to the school website is only permitted with parental permission.

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, they would be encouraged to report incidents to the Headteacher and unions.

E-mail Use

The school should have e-mail addresses for children and young people to use as a class as part of their entitlement to being able to understand different ways of communication and using technology to share and present information in different forms.

The school may occasionally set up e-mail addresses for individual children and young people to use, as part of a specific project related to the school curriculum.

School staff should use their school issued e-mail addresses for communications related to school business.

Mobile Devices (including Mobile Phones and any other Emerging Technologies)

(i) Personal Mobile Devices

- Staff must not use their personal mobile devices in school, except before school starts/at break time/at the end of the school day, unless agreed in advance with the Headteacher (e.g. SPLSAs).
- When not in use, staff personal mobile devices must not be kept on their person and should be kept in a locker (where available) or in their classroom cupboard (that pupils do not have access to). Mobile devices can also be kept in the main office, Headteacher's office or Deputy Head's office.
- Staff must not use their personal mobile devices when pupils are present, unless agreed in advance with the Headteacher (e.g. SPLSAs).
- Staff must not use their personal mobile devices to take photos or videos of pupils under any circumstances.
- Staff must not use their personal mobile devices to make calls to pupils or to send messages to pupils.
- Staff must not give their home telephone number or their personal mobile phone number to pupils and are advised against giving their phone numbers to parents / carers.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

(ii) 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 establishment has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, this equipment should only be used to conduct school business, except as allowed for in the Personal Use and Privacy section of this policy.
- Personal or family use of school cameras and video/audio recording equipment is not permitted.
- Staff must not send any images of pupils to anyone.

Games Consoles

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. Before use within school, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.

Video and Photographs

The term ‘image’ refers to the taking of video footage or photographs via a camera or other technology e.g. mobile phone.
Staff may only take and store ‘images’ of pupils on school issued equipment.

Volunteers/students on work experience must not take ‘images’ of any pupils, except on school equipment at the request of the class teacher.

Any ‘images’ should only be used in school to support pupils’ learning and must not be uploaded to the internet without parental permission.

Other visitors/professionals wishing to take any ‘images’ of pupils must have permission from the school. ‘Images’ must not be sent to anyone or uploaded to the internet, without parental permission.

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 pupils should only be used after permission has been given by a parent/carer.

Video-Conferencing and Webcams

Video conferencing and web cams are not currently used as tools for learning at Hillside and so the following is for information only at present. Should the school make use of these tools in the future, this statement will be amended accordingly.

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 supervised by a member of staff and a record of dates, times and participants held by the school.

Managing Social Networking and Other Web Technologies

Social networking sites have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service offers users both a public and private space through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed.

With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, MySpace and Bebo.)

Social Networking Advice for Children and Young People

Whilst pupils at Hillside are not allowed access to social networking sites using school equipment or whilst at school, it is recognised that some children and young people may access these sites elsewhere.

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

- Pupils should be discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school/education setting or other establishment uniform).
- 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.

Social Networking Advice for Staff

(to be read in conjunction with Policy and Guidance on the Use of Social Networking Sites)

Social networking outside of work hours, on non school 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. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent pupils from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in any personal online contact with pupils.
- Staff are strongly advised against accepting parents as 'friends' on their social networking site.
- Staff should ensure that full privacy settings are in place to prevent pupils or parents from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine.
- Photographs taken in relation to all school activities must not be placed online or on any social networking site.

Safeguarding Measures – Filtering

The school uses the E2BN broadband connectivity and its associated filtering system which is set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. All filtering is set to 'No Access' within any setting and then controlled via:

- Portal Control (controls filtering at local site level) which controls individual access to the internet. This also links to the E2BN criteria 'Schedule 11' of Level Four site filtering to qualify for access to the broadband services.
- Local Control – controls access to websites and provides the option to add to a 'restricted list'.

The learning platform is set within a filtering service that will provide the same level of protection for all users.

Anti-virus and anti-spyware software is used on all network and stand alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about children and young people and the school cannot be accessed by unauthorised users.

Links or feeds to Online Safety websites are provided. 'Hector Protector' should be used as a screen cover so that anything accidently accessed can be covered whilst an adult is informed.

CEOP (Child Exploitation and Online Protection Centre) training is used in conjunction with the PSHE curriculum for raising awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is available for further advice and information on children or young people's personal online spaces. There is an Online safety Trainer in school, who delivers annual update training to all staff.

Tools for Bypassing Filtering

Staff are forbidden to use any technology designed to circumvent, avoid or bypass any school security controls (including internet filters, antivirus solutions or firewalls) as stated in the Online Safety and Acceptable Use of ICT rules for staff, governors and visitors.

Violation of this rule will result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

Monitoring

The Online Safety Lead / Deputy Head should be monitoring the use of online technologies by children and young people and staff, on a regular basis.

Teachers should monitor the use of the internet during lessons.

Parents/Carers – Roles

Parents/carers should be sent a letter requesting permission for their child to use the internet in school. This should be signed and returned to the school, and kept on record.

Support

As part of the approach to developing Online Safety awareness with children and young people, the school should offer parents the opportunity to find out more about how they can support the school in keeping their child safe and find out what they can do to continue to keep them safe whilst using online technologies beyond school. School will do this through distribution of information leaflets and by holding e-Safety awareness sessions for parents/carers.

Links to Other Policies

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

All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all Computing and PSHE materials for children and young people and their parents/carers. People should not treat

online behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour.

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 allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Headteacher/Senior Designated Person for safeguarding within the school immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations:

The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

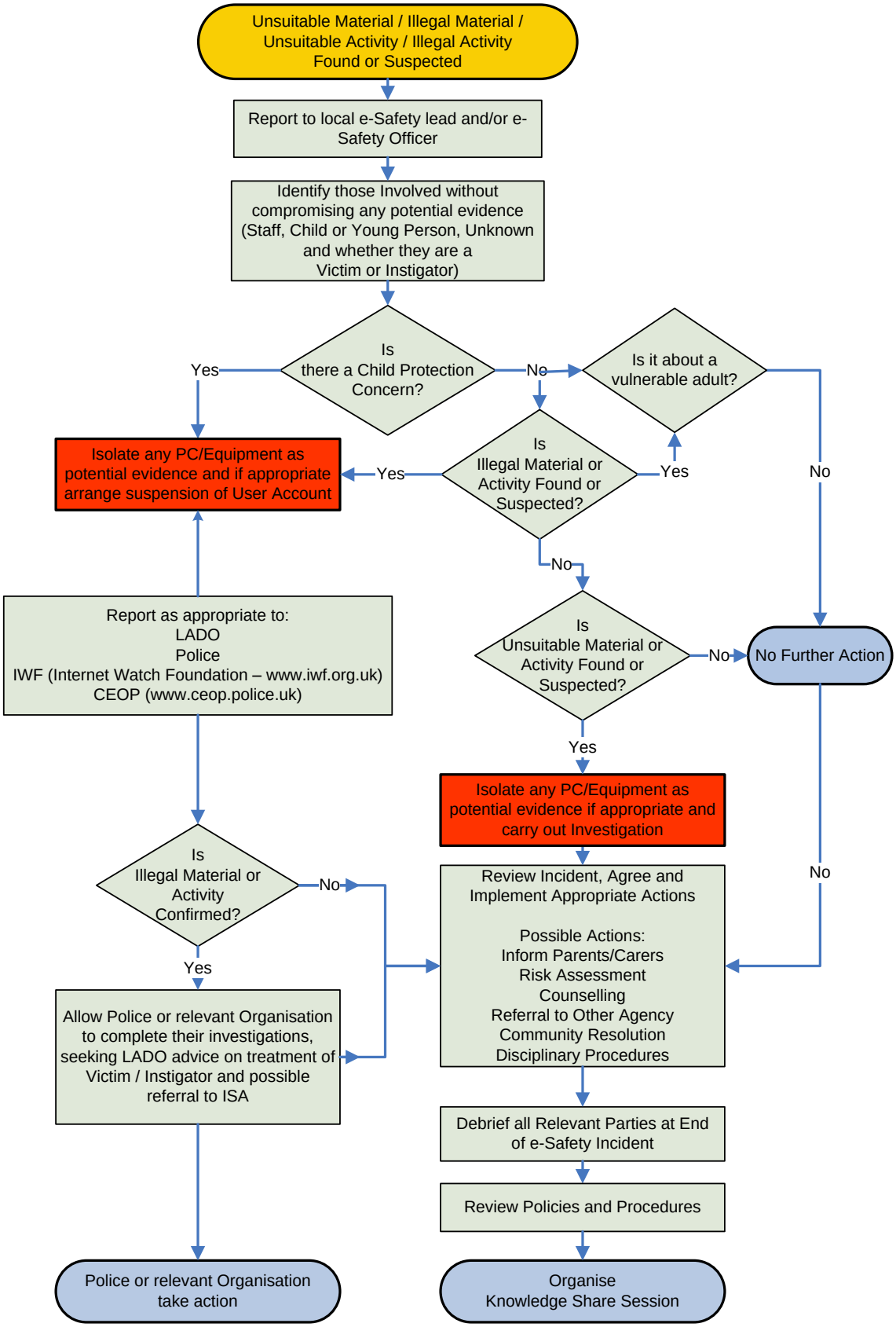
Curriculum Development

The teaching and learning of Online Safety should be embedded within the PSHE curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line.

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.

Fig 1: Online Safety FlowChart



Online Safety and Acceptable Use of ICT Agreement for Staff, Governors 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. They are asked to sign this Online Safety and Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I know that images (video or photographs) and/or personal information of children and young people must **not** be uploaded to the internet.
- I have read the procedures for incidents of misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Headteacher/ Designated Safeguarding Lead or Online Safety Lead in accordance with procedures listed in the Online Safety and Acceptable Use Policy.
- I know who my Designated Safeguarding Lead is.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher and/or Online 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 Online 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 read, understood and agree with this Agreement as I know that by following them I have a better understanding of Online Safety and my responsibility to safeguard children and young people when using online technologies.

Signed …… Date ……

Name (printed)……

Summary of Online Safety Advice for Staff

This is to help keep everyone safe when using the internet and other portable devices.

DO	read the Online Safety and Acceptable Use Policy (displayed in the staffroom and available from school office).
DO	keep your personal mobile device in a locker (where available) or in your classroom cupboard (that pupils do not have access to), whilst working with pupils. Mobile devices can also be kept in the main office, Headteacher's office or Deputy Head's office.
DO	keep your professional and personal information and images separate.
DO	remember that anything posted online is available to **anyone in the world**.
DO	only use school cameras for school photographs.
DO	guide pupils to appropriate materials when using the internet.
DO	supervise pupils at all times when using the internet.
DO	report any inappropriate use or websites to Deputy Head/Online Safety Lead immediately.
DO	use the school email address given to you.
DO	keep all portable storage devices in school. Teachers may take these home to undertake school related work in the evenings or at weekends but they should never be left at home.
DO	ensure that your portable devices are password protected or encrypted.

DO NOT	use your personal mobile devices in school, except before school starts/at break time/at the end of the school day, unless agreed in advance with the Headteacher (e.g. SPLSAs).
DO NOT	use your personal mobile devices when pupils are present, unless agreed in advance with the Headteacher (e.g. SPLSAs).
DO NOT	take photographs or recordings of pupils on your personal mobile devices.
DO NOT	send images of a pupil to anyone or upload such images to a social networking site.
DO NOT	use your personal mobile devices to make calls to pupils or to send messages to pupils.
DO NOT	use school equipment (e.g. cameras or video recorders) for your personal or family use. The school permits very limited personal use of laptops by authorised users as stated in the Online Safety and Acceptable Use Policy.
DO NOT	access social networking sites from the school ICT facilities.
DO NOT	leave your profile open or unattended.
DO NOT	retrieve, copy, send or display offensive messages or pictures.
DO NOT	harass, insult or attack others.
DO NOT	publish, share or distribute personal information about a pupil/family or member of staff.
DO NOT	use another person's password.
DO NOT	download software without first consulting the Deputy Head/Online Safety Lead.
DO NOT	allow pupils to access a computer in school using your profile.
DO NOT	try to access: pornographic or "top shelf" adult material; images of children or adults that could be considered inappropriate; material that has gratuitous violence, injury or death in it; material likely to lead to the harassment of others; materials promoting intolerance or discrimination; materials relating to criminal or unlawful activity; materials that may generate a security risk.
DO NOT	violate copyright laws.
DO NOT	subscribe to any services or order any goods/services unless specifically approved by school.
DO NOT	use school ICT facilities for any commercial activity.

Online Safety Checklist

Is your school community online safe?

Does your school …	
✓ *if appropriate*	
	have a nominated Online Safety Lead?
	have the necessary acceptable use policies?
	check that appropriate Online safety procedures and practices are in place and working?
	use an accredited supplier for internet services?
	include Online safety as part of your internet services?
	keep a log to record and monitor Online safety incidents?
	raise awareness of Online safety issues by holding workshops and events?

Do all your staff and helpers…..	
✓ *if appropriate*	
	understand Online safety issues and risks?
	receive regular training and updates?
	know how to support youngsters with new technologies?
	know how to report and manage issues or concerns?
	know how to keep data safe and secure?
	know how to protect and conduct themselves professionally online?
	take the opportunity to consult with youngsters?

Do your youngsters ……	
✓ *if appropriate*	
	understand what safe and responsible online behaviour means?
	get opportunities to learn about Online safety?
	get the opportunity to improve their digital literacy skills, e.g. how to search safely and effectively online?
	Know the SMART rules?
	get the opportunity to give their views about staying safe on line?
	know how to report any concerns they may have?

Can you help parents and carers ……	
✓ *if appropriate*	
	understand Online safety issues and how to manage risks?
	understand their roles and responsibilities?
	receive regular training and updates?
	understand how to protect their children at home?

Dear Parent or Carer

Parental permission for child to use the internet in school

During Computing and other curriculum studies, your child may, on occasions, be given the opportunity to use the internet. Our system is extremely well protected to prevent access to any unsuitable information or images. Children are always closely supervised when working online and staff are aware of the need to remain vigilant at all times.

Please return the slip below to indicate whether you give permission for your child to use the internet at school.

If at any time, you have concerns please do not hesitate to contact Shelley Jackson (Online Safety Lead).

Yours faithfully

Michelle Kelly
Headteacher

- -

F.A.O. Hillside School Office

Parental permission for child to use the internet at Hillside Special School

I give / do not give permission for …….. (child's name) to use the internet at school. I understand that internet access is restricted and that children are closely supervised at all times.

Signed: …….

Parent/Carer's Name: …….

Date: …….