

All Saints' CEVCP School



eSafety Policy

Inspire Challenge Succeed

Review Frequency	Every 3 years	Approval Level Required	Full GB
Approved by:	Full GB	Approval Date:	09/02/2017
Signed:		Print Name:	Richard Harding Chair of Governors

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 the school 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' 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 the school setting.
- 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 setting.
- 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/ Headteacher/Management Committee Members

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

Motivation Cooperation Creativity Independence Curiosity Stickability

- The Headteacher has designated an eSafety Lead (Clare Lamb, the Headteacher)) to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment. All staff and pupils are aware of who takes this role within the school setting.
- Resources should be provided for the eSafety Lead and staff to be trained and update policies, where appropriate.
- The Headteacher 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 Headteacher should inform the Governors at the Curriculum meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to safeguarding. 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 setting. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.
- An e-Safety Governor (Kerry Wigg, the Safeguarding Governor) will jointly monitor all related policies, including the Acceptable Use Policy and Anti Bullying/ Cyber Bullying policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:
Challenging the school setting about having:
 - 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.
- 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.

Local eSafety Lead

It is the role of the designated eSafety Lead to:

- Appreciate the importance of e-safety within the school setting 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 setting.
- Ensure that the AUP (Acceptable Use Policy) is reviewed annually, with up-to-date information and that training is available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Check 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.
- 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/Manager on a regular basis.
- Liaise with the PSHE, safeguarding and ICT 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 e-safety information can be taught or adhered to.
- 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.
- Ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone 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-alone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised. Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, where:
 - Blanket e-mails are discouraged
 - Tone of e-mails is in keeping with all other methods of communication

Staff or Adults

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

- Ensure that they know who the Senior Designated Person for Safeguarding is within the school setting so that any misuse or incidents can be reported which involve a child.
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher/Senior Designated Person. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Anti-bullying/ Cyber Bullying Policies 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/Senior Designated Person 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 e-Safety Lead.
- Alert the e-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 e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the school setting, 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 station unattended when they or another user is logged in.
- To ensure that the Senior Office Administrator follows the correct procedures for any data required to be taken from the school setting.
- Report accidental access to inappropriate materials to the e-Safety Lead in order that inappropriate sites are added to the restricted list or control this with the Local Control options via the school's 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) that 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.

Children and Young People

Children and young people should be:

- Responsible for following the Acceptable Use Agreement whilst within the school setting as agreed at the beginning of each academic year or whenever a new child attends the school setting for the first time.
- Taught to use the Internet in a safe and responsible manner through ICT and/or PSHE lessons.
- 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).

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.

They 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.

All staff should read the Acceptable Use Policy and the Acceptable Use Agreement, which they need to sign and return to the school to keep under file.

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.

In the Event of Inappropriate Use by Staff or Adults

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 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.

Appropriate and Inappropriate Use by Children or Young People

Acceptable Use Agreements and the letter for children, young people and parents/carers are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within the school setting including downloading or printing of any materials. 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, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so. The agreement should be on display within the classrooms and the computer suite.

The school should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreement together so that it is clear to the school that the child or young person, with the support of the parent/carer, accepts the agreement. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond the school setting.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

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.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using them in or beyond the school setting.

In the Event of Inappropriate Use by Children and Young People

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.
- The incident will be recorded on the school's safeguarding incident report, updated January 2017.
- 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.

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 so that an adult can take the appropriate action. 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.

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

The Curriculum and Tools for Learning

Internet Use

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 4:

- 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.

Our ICT Scheme of Work is used to teach Internet and E-mail lessons from Years 1 to 4. e-Safety lessons and resources can also be found at www.thinkuknow.co.uk for KS1 and KS2.

These skills and competencies are taught within the curriculum 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. Children and young people should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

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.
- Name of 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.

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.

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.

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 ought to 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.

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, the school is encouraged to report incidents to the Headteacher, using the reporting procedures for monitoring.

E-mail Use

The school has email addresses for children and young people to use as a class, 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 only. 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 and young people is to communicate 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 on a regular (weekly or as necessary) basis.

Mobile Phones and Other Emerging Technologies

The school should carefully consider how the use of mobile technologies could 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 the school's filtering and allow access to inappropriate or potentially harmful material or communications.*

Mobile phones brought in to school by pupils will be left in the school office. A letter will be required from parents explaining the reasons why their child needs to have a mobile phone with them during school hours.

(I) Personal Mobile Devices

Staff should be allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people 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. Before use within the 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.

(ii) School/Education Setting or Other Establishment 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 business outside of the school setting.

It should also be policy to ensure that children and young people understand the use of a public domain and the consequences of misuse. Relevant curriculum links should be made to highlight the legal implications and the involvement of law enforcement.

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 the school setting there is access to:

Class digital cameras

It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.

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 and young people in a forum or using Instant Messaging within the learning platform should be 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 young people and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. The school will need to decide how photographs will be used, including where they will be stored (central location which could be viewed by anyone) and when they will be deleted.

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.

Video-Conferencing and Webcams

Flashmeeting is the main video conferencing service provided by E2BN which allows staff to pre-set 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 the school setting.

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 setting. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

Managing Social Networking and Other Web 2.0 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.)

Motivation Cooperation Creativity Independence Curiosity Stickability

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.
- Pupils are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, IM and email address or full names of friends).
- Pupils are 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 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 allowing for the procedures, as set out in the anti-bullying policy, to be followed.

Social Networking Advice for Staff

Social networking outside of work hours, on non-school 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 personal online contact with pupils outside of Headteacher authorised systems (e.g. school email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent pupils 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 (avoiding fake profiles set up by pupils).

Safeguarding Measures – Filtering

Staff, children and young people are required to use the personalised learning space and all tools within it, in an acceptable way. Please refer to the Acceptable Use Agreement for Staff and children and young people for the appropriate use of the learning platform.

The E2BN broadband connectivity has a filter system, which should be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. **All** filtering should be 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 levels listed below are in relation to age-appropriate categories:

Level One	E2BN standard basic minimum adult policy.
Level Two	E2BN standard senior pupils' policy.
Level Three	E2BN standard younger pupils' policy.
Level Four	E2BN standard young pupil's policy. No search, no politics and religion.

This complies with the agreed connectivity legalities with Synetrix and E2BN and also ensures our younger audiences are not exposed to unnecessary risks e.g. a blanket Level Two for Primary school users is inappropriate.

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 standalone 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.

The 'skin' of the online personal space is age appropriate and only tools appropriate to the age of the child are available.

Links or feeds to e-safety websites are provided. For older children and young people, the Report Abuse button is available should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and Online Protection Centre) children is annual and part of the ICT and/or PSHE curriculum for raising awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is part of the skin layout for further advice and information on children or young people's personal online spaces.

Monitoring

The e-Safety Lead should be monitoring the use of online technologies by children and young people and staff, on a regular basis. This is done through annual pupil and parents surveys and during OHSE and IT lessons.

Teachers should monitor the use the Internet during lessons and also monitor the use of e-mails from the school setting and at home, on a regular basis.

Parents – Roles

Each child or young person should receive a copy of the Acceptable Use Agreement on an annual basis or first-time entry to the school setting which needs to be read with the

parent/carer, signed and returned to the school confirming both an understanding and acceptance of the agreement.

It should be expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted. The school should keep a record of the signed forms.

Support

As part of the approach to developing e-safety awareness with children and young people, the school offers parents information and guidance 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 the school setting. The school wants to promote a positive attitude to using the internet and therefore wants parents to support their child's learning and understanding of how to use online technologies safely and responsibly. The school will do this by holding an e-safety Parent/Carer Information Evenings and providing a range of resources on the school website.

Resources

The school:

- Can use the Child net International 'KnowITAll for Parents' online materials (<http://www.childnet-int.org.uk/kia/parents/cd/>) to deliver key messages and raise awareness for parents/carers and the community.
- The Parents section of the school website contains a range of resources to support parents.

Links to Other Policies - Behaviour and Anti-Bullying Policies

Please refer to the Anti-bullying/ Cyber-bullying 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 ICT 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. This is a key message which should be reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

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 Senior Designated Person (SDP) for safeguarding within the school setting immediately. In the event of an allegation being made against a Head teacher, 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 Settings

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

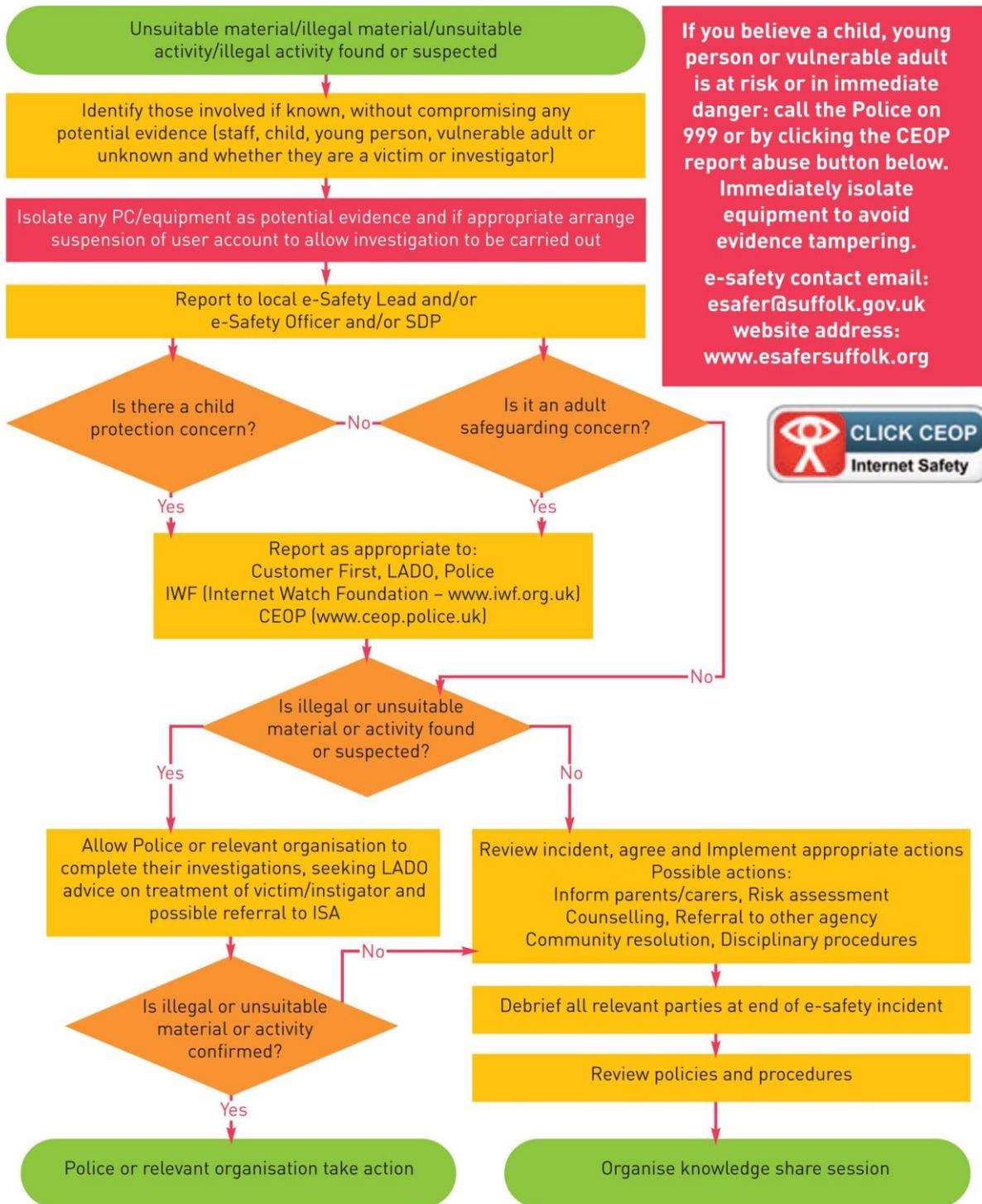
The teaching and learning of e-Safety should be embedded within the school curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line. This may form part of the PHSE module but is not exclusive to this area of curriculum and opportunities to embed e-Safety throughout the curriculum should be sought.

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: e-Safety Flow Chart

e-Safety Incident Flowchart



If you believe a child, young person or vulnerable adult is at risk or in immediate danger: call the Police on 999 or by clicking the CEOP report abuse button below. Immediately isolate equipment to avoid evidence tampering.

e-safety contact email: esafers@suffolk.gov.uk
 website address: www.esafersuffolk.org





Acceptable Use 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 All Saints' CEVCP 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 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's 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 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, Senior Designated Person or e-Safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- 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's 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 Policy to refer to about all e-safety issues and procedures that I should follow.
-

I have read, understood and agree with these Agreement as I know that by following them 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:

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.

Signed: Dated:

Name:(Printed)