East Hunsbury Primary School

E- Safety and Acceptable Use Policy

E-Safety and Acceptable Use Policy

Statement of Intent

Introduction

We believe…

- Our school should be a stimulating and welcoming community in which all children and adults feel valued, able to contribute and where relationships are based on mutual respect.

- Children should be active participants in the learning process and be provided with experiences that maximise their involvement, autonomy and independence.

- We should be an inclusive community where pupils are offered opportunities to grow together, learn together, laugh together and celebrate together.

- We should equip our children with the skills they need to be happy and successful in life, nurturing in them a true and lifelong love of learning.

- We are responsible for the development of the whole child. We recognise differing needs and endeavours to meet these needs, maximising the opportunities for children to explore their physical, social, emotional and intellectual potential.

- We should be a community that respects and celebrates diversity.

Our school is committed to achieving the five required outcomes of the Children Act 2004 ('Every child Matters'), i.e. that all children:

- Be healthy;
- Stay safe;
- Enjoy and achieve;
- Make a positive contribution;
- Achieve economic well-being.

The Governing Body has set in place:

(i) Appropriate arrangements for ensuring a safe and healthy working and learning environment is provided

(ii) A monitoring and evaluation system to ensure the policy is being met.

What is an AUP (Acceptable Use Policy)?

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within our school. The policy recognises the ever changing nature of emerging technologies within the curriculum and media and highlights the need for regular review to incorporate development within Computing. At present the internet technologies used extensively by young people in both home and school environments include:

- School websites/blogs
- Social Networking
- Gaming/forums
- Music Downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Office 365
- Skype
- Video Broadcasting
- Apple/Windows apps

This policy provides support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It also explains procedures for any unacceptable use of these technologies by children or young people, and refers to school disciplinary procedures for staff.

Why have an AUP?

The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies. The risks include:

- Spam and other inappropriate e-mail.
- Online grooming.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device.
- Viruses.
- Cyberbullying.
- The sending of indecent personal images, videos or text via mobile phones for private viewing.
- On-line content which is abusive or pornographic.
- Radicalisation and other religious movements.
- Social and emotional effects of an increased use of technology.

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks. Where possible, another member of staff should be copied into emails to also reduce risks. There is also a responsibility to educate parents about the risks and how this is managed inside of school, along with what they can do at home to help safeguard their child. As part of the 'Every Child Matters' agenda set out by the government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure children and young people continue to be protected.

Aims

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 or other educational settings.

- To provide safeguards and rules for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults, including parents, are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures.

Organisation for Implementing the Policy

Roles and Responsibilities:

The e-Safety Leads for East Hunsbury Primary School are:

- Alex Bartosiak-Smith (Deputy and Safeguarding Lead)
- Kelly Robinson (Computing Lead)
- Suzanne Andrews (Safeguarding Governor)
- Phil Sugars (Curriculum and Computing Governor)

The Senior Designated Safeguarding Leads are:

- Alex Bartosiak-Smith – Deputy Headteacher
- Lucy Ingman – Assistant Headteacher and SU Manager

Deputy Designated Safeguarding Leads

- Rita Arundel - Headteacher
- Julia Fenton – Assistant Headteacher

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Headteachers

- The Headteacher has designated to the Senior Safeguarding Leads and Computing Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately. All staff and students are aware of who holds these post within the school.
- Time and resources are provided for the e-Safety Leaders and staff to be trained and update policies, where appropriate.
- The Headteacher, Deputy Headteacher and Computing Lead promotes e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Deputy Headteacher will inform the Governors at Safeguarding Committee meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure they know how this relates to child protection.
- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Computing Lead.

- The Headteacher and Lead Designated Safeguarding Leads should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. They will receive regular information about online safety incidents and monitoring reports via the Safeguarding committee.

- The Governors must ensure that E-Safety is embedded within Safeguarding training, guidance and practices.
- A Safeguarding Governor has been elected to challenge the school about any concerns and procedures

Computing Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the safeguarding lead to liaise with the Local Authority / relevant body
- Liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- reports regularly to Senior Leadership Team
- Update the AUP bi-annually and share it with staff and parents where appropriate.
- Ensures that policies and procedures are updated and take into account any emerging issues and technologies.
- Co-ordinates or delivers staff training according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Implements a system of monitoring staff and pupil use of school issued technologies and the internet, where appropriate. This will be done by monitoring issues when concerns are raised.
- Trains staff on how to log an e-Safety incident.
- Looks at and monitor how E-Safety is taught throughout KS1 and KS2 to ensure coverage in line with the government and OFSTED guidance.

Technical staff:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any Local Authority / Academy Group / other relevant body Online Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet / Learning Platform / remote access/ email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Computing Lead for investigation.
- That monitoring software / systems are implemented and updated as agreed in school / academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school / academy Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Senior Designated Safeguarding Lead for investigation.
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Students / pupils understand and follow the Online Safety Policy and acceptable use policies
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

- Makes staff aware of the Safeguarding Procedures at www.proceduresonline.com/northamptonshire/scb/

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Students / Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's / Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website / Learning Platform
- Their children's personal devices in the school (where this is allowed)
- E-Safety Parent/Carer Information Sessions will be held annually to raise awareness of key internet safety issues and highlight safeguards currently in place at school (e.g. filtering and training in place to minimise online risk.)
- Free to order resources from Childnet (http://www.childnet-int.org/kia/parents/) and the Thinkuknow website (http://www.thinkuknow.co.uk/teachers/resources/) can be used to support this. Wherever possible, the school will endeavour to provide internet access for parents/carers without this resource at home to ensure that appropriate advice and information on this topic can be viewed.

Appropriate and Inappropriate Use

By staff or adults

To ensure that both young people and staff are appropriately safeguarded against online risks and allegations, a copy of the Acceptable Use Policy/Code of Conduct will be made accessible to all. The policy clearly highlights any behaviours or practices, linked to staff use of technologies, which are deemed inappropriate by HM Government 'Safer Working Practice' guidelines or other relevant safeguarding legislation and professional standards. Staff are expected to take responsibility for their own use of technology and are asked to read and sign acceptance of the staff acceptable use rules annually.

Examples of inappropriate use:

- Accepting or requesting current or past pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers.
- Behaving in a manner which would lead any reasonable person to question a staff member's suitability to work with children or act as a role model. This would include inappropriate comments, photographs or videos on social networking sites which reflect badly on either the individual, their colleagues or the school/workplace. In the event of inappropriate use If a member of staff is believed to misuse the internet or learning platform in an illegal, inappropriate or abusive manner, a report must be made to the Headteacher/Safeguarding Lead immediately and the appropriate allegation procedures and child protection policies must be followed to deal with any misconduct and all relevant authorities contacted. In the lesser event of minor or accidental misuse, internal staff disciplinary procedures will be referred to in terms of any action to be taken.

By Children or Young People

Children are clearly guided in E-safety lesson as to the appropriate use of the internet and technologies. If a child or young person is found to misuse online technologies or equipment whilst at school, the following sanctions will apply:

- Deliberate misuse of the internet/technologies will result in a letter being 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 rules may result in withdrawal of a student's internet privileges for a period of time and another letter 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 of accidental access to inappropriate materials, students are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action.
- In the event of a member of staff being aware of a child having a Facebook/ twitter account, a letter will be sent home to their parents informing them of this and reminding them of the legal age requirement. Appropriate E-Safety incident procedures are then followed.

The Curriculum

Internet use - It is the responsibility of schools to teach their students how to use the internet safely and responsibly. The following concepts, skills and competencies will be developed through both the PSHE and ICT curriculum:

- Internet literacy
- Making good judgements about websites and emails received
- Knowledge of risks such as viruses and opening mail from a stranger
- Knowledge of copyright and plagiarism issues
- File-sharing and downloading illegal content
- Uploading personal information – what is and is not safe
- Where to go for advice and how to report abuse.

It is also the schools' responsibility to plan in opportunities for children to make informed judgements and manage risks themselves rather than relying on filtering systems. Online personal safety is taken extremely seriously within our school community and our students are encouraged to refrain from sharing personal information in any form of electronic communications. Personal informal includes:

- full name
- address
- telephone number
- email address

Pupils with additional learning needs - The school strives to provide access to a broad and balanced curriculum for all learners and recognises 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.

Email use

Students

The school has set up individual class email addresses for students to use as a class, as part of their entitlement to understand different ways of communicating and using ICT to share and present information. Students will use this email account for any form of school related communications (i.e. homework) and teaching staff will regularly monitor their class use of these systems. Teachers may want to pass this on to parents as a form of communication. Children's emails are set as their first initial and second name followed by the school. If there are any cases where a child (for safeguarding purposes) cannot use this set up, alternative options should be offered, such as the email being turned off or directed to the class teacher. They should not use this email to sign up for any other sites.

Staff

Professional email addresses will be used for all electronic correspondence between staff and students, and for school related business only. This is true also for any communications with parents or carers. Under no circumstances will staff members engage in personal communications (i.e. via hotmail or yahoo accounts) with current or former students outside of authorised school systems. The use of professional email accounts allows for content monitoring to take place and minimises the risk of allegations being made against staff.

Mobile technologies

Everyday technologies, including mobile phones, mp3 players, tablets are increasingly being used by both adults and children within the school environment. For this reason, appropriate safeguards must be in place to protect young people and staff against the following associated risks:

- Inappropriate or bullying text messages
- images or video taken of adults or peers without permission
- Videoing violent, unpleasant or abusive acts towards a peer or adult which may be distributed
- 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
- All teachers have their own year group mobile devices to use when taking photos. No personal devices or mobile phones should be used for this. Devices are regularly monitored and wiped clear throughout the academic year.

Mobile phones Student Use:

Students are advised NOT to bring mobile phones to school. If there is no alternative, they are kept by the class teacher's drawer. If there is reason to suspect that a student's mobile device contains inappropriate, illegal or harmful content, whilst on school grounds, it will be confiscated by staff and may be searched. The e Safety Incident and Child Protection procedures will be followed if such content is discovered.

Staff Use:

Staff may bring personal mobile phones into school, but they will be used outside of lesson time only. Under no circumstances will staff use their personal mobile phone to communicate with current or former students. School telephone numbers or mobile phones will be used for this purpose, apart from when on off-site school trips. All images or video recordings of children and young people will be taken using school equipment, never personal camera phones or other such devices. It is the responsibility of staff to ensure that no inappropriate or illegal content is stored on their device when bringing it onto school grounds.

Laptops/Tablets:

Teaching staff are provided with school laptops/tablets to allow for school related work to be completed off site. Personal use of school issued computing facilities is permitted providing it is kept to a minimum and does not interfere with the employee's work. Sensitive data and school authorised images of students should not be stored on school laptops. In the event that a laptop/tablet is stolen or lost there is potential for this content to be viewed by unauthorised individuals. This applies also to the use of memory sticks for transferring information between school and home.

Video and photographs

Images or videos featuring students will only feature on the school website or in press coverage if permission has been granted by parents/carers in advance. Wherever possible group shots of children will be taken, as opposed to images of an individual and first names only will be displayed. Photographs should not show children in compromising positions or in inappropriate clothing (e.g. swimming costumes). School equipment will be used to take any images of students, and pictures should be removed from cameras and utilised appropriately within 24 hours of being taken. This is to ensure that images of students cannot be viewed by unauthorised individuals in the event of loss or theft.

Video-conferencing and webcams

To safeguard staff and young users, publicly accessible webcams are not to be used in school. As with video and photographs, permission will be sought from parents/carers before a child engages in video conferencing with individuals or groups outside of the school setting. All video conferencing will be supervised by staff and a record of dates, times and participants held in school for audit trail purposes.

Managing Social Networking and other Web 2.0 technologies

Social networking is now the communication form of choice for many adults and young people worldwide and, as a result, safeguards must be in place to ensure that staff and students are aware of the risks associated with this form of technology. To address this issue, a series of preventative measures are in place.

- Access to social networking sites is controlled through the school internet filtering systems. In KS2, Yammer may be used for classes to share information. This should remain a closed domain and no external people should be invited to the group.
- Children to avoid direct messaging teachers and instead post on the threads. Teachers are to regularly monitor use and plan in

opportunities for children to explore the benefits of social media within a controlled and safe environment.

- Students and staff are discouraged from providing personal details or identifiable information on profiles (e.g. mobile number, address, school name, clubs attended, email address or full names of friends).
- Children are encouraged to include images of avatars for their display icon instead of real pictures.
- Students and staff are made aware of the risks of posting images online and how publicly accessible their content is. Background images in photographs which may reveal personal details are also addressed (e.g. house number, street name, school uniform)
- Social networking security settings are explained 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.
- Comments on the blogs are regularly monitored, with the teacher modelling appropriate responses which should be left.
- Both online and school systems for reporting abuse or unpleasant content, i.e. cyberbullying, are reinforced www.thinkuknow.co.uk.

Staff using social networks

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, staff have a responsibility to ensure that their actions outside of school do not impact on their work with children and young people. HM Gov ‘Safer Working Practice’ clearly states that adults working with children should:

- Only make contact with students for professional reasons and with the authorisation of the Headteacher.
- Any communication should be via professional email only and never through a personal email account.
- Ensure that if a social networking account is used, details are not shared with children and young people and privacy settings are set to a maximum.
- Be aware that behaviour in their personal lives may impact on their work with children and young people.
- Not behave in a manner which would lead any reasonable person to question their suitability to work with children and young people.

Safeguarding measures

Under the Counter-terrorism and Security Act 2015, which came into force on 1 July 2015, there is a requirement that schools “have due regard to the need to prevent pupils being drawn into terrorism.” The school uses Surf Protect via Exa which is installed into all child devices in the school. This software detects key words which are either typed in, or appear on the screen. An image is taken of the screen and logged in the central system. The device, year group, time and content is then listed. Weekly monitoring takes place, with each ‘hit’ being reviewed and categorised. Any further action required is done so by the E-safety lead. Repeated incidents are logs to form a history if needed.

Filtering

The Exa networks filtering system provides a filtered internet service to East Hunsbury Primary which prevents access to illegal and inappropriate sites. The school has access to a local control list which allows websites to be added to a 'restricted list'. Changes to the filtering will be agreed by the Headteacher and Computing Lead, these changes will be implemented by the school's IT support company. In addition to the above, the following safeguards are also in place:

- Annually, the Headteacher will sign a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband by Exa Networks.
- Reports can be produced from the school's filtering system, SurfProtect, which show what websites and search queries have been blocked.
- 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 to e-safety websites are provided on the school website.
- Encryption codes on wireless systems.

School website

- Permission will be sought from parents/carers prior to the uploading of any images onto the school website. Consideration is given to which information is relevant to share with the general public on a website and secure areas will be used for information pertaining to specific audiences. The schools AUP will also be published on this platform along with recommended websites.

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:
An inappropriate website is accessed inadvertently:

- Report website to the Computing Lead if this is deemed necessary they will add this site to the banned list immediately.
- An inappropriate website is accessed deliberately or an adult has used ICT equipment inappropriately:
- Ensure that no one else can access the material by shutting down.
- Log the incident.
- Report to the Senior Designated Lead and Computing Lead immediately.
- Senior Designated Lead to refer back to the Acceptable Use Rules and follow agreed actions for discipline.

An adult receives inappropriate material.

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Headteacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police.

An adult has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately, if necessary.
- Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
- Contact CEOP (police) as necessary.

Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:

- Preserve any evidence.
- Inform the Headteacher immediately and follow Child Protection Policy as necessary.
- Inform the Computing Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Headteacher.

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

An inappropriate website is accessed inadvertently:

- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the Computing Lead if this is deemed necessary.
- ICT lead will add site to the banned list immediately.

An inappropriate website is accessed deliberately:

- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.

An adult or child has communicated with a child or used ICT equipment inappropriately:

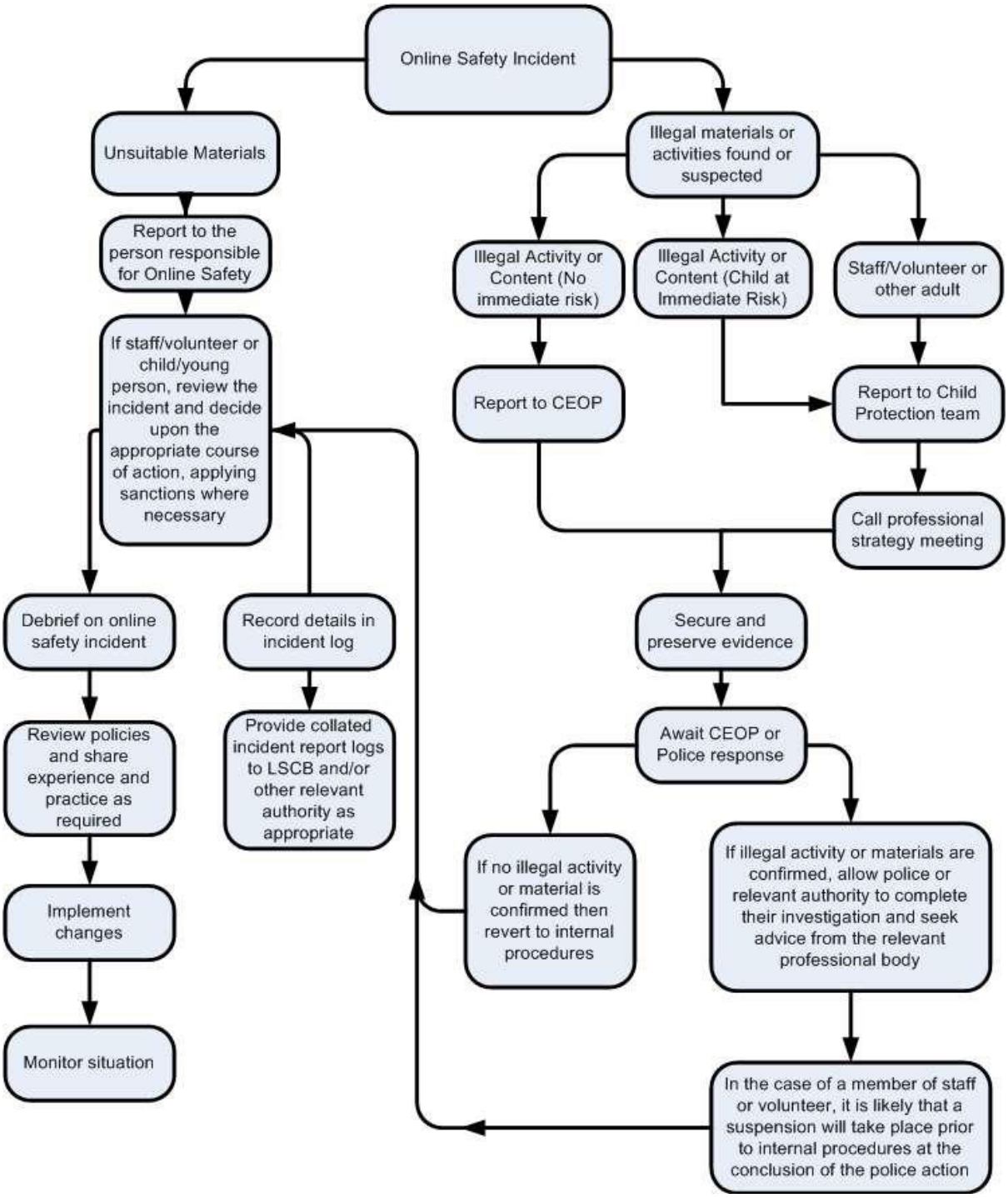
- Ensure the child is reassured and remove them from the situation immediately.
- Report to the Headteacher and Designated Person for Child Protection immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy Contact CEOP (police) as necessary.

Threatening or malicious comments are posted to the school website or learning platform about a child in school:

- Preserve any evidence.
- Inform the Headteacher immediately.
- Inform the Computing Lead so that new risks can be identified.
- Contact the police or CEOP as necessary.

Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence.
- Inform the Headteacher immediately. N.B. There are three incidences when you must report directly to the police.
- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child. CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine. Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image. www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line. Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board Northamptonshire guidance. All adults should know who the Designated Person for Child Protection is. It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action