Hook Infant School

E-Safety Policy

2021-2024

Contents

Appendices

Development, Monitoring and Review of this Policy

This e-safety policy has been developed by the following staff:

- The Headteacher
- Deputy Head
- Computing Coordinator
- Data Protection Officer

Consultation within the school community has taken place through Parentmail communication, online surveys, informal drop in sessions and with an 'open door' policy for parents and community.

Schedule for Development, Monitoring and Review

This e-safety policy was approved by the Governing body on:	**See Page 14**
The implementation of this e-safety policy will be monitored by the:	**Data Protection Officer**
Monitoring will take place at regular intervals:	**Real time: HPSN2, Smoothwall** **Manual checks: Half Termly**
The E-Safety Policy will be reviewed every three years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	**Autumn Term 2024**
Should serious e-safety incidents take place, the following external agencies should be informed:	**LA Safeguarding Officer** **Police** **www.ceop.police.uk**
Should any data breaches occur as a result of an e-safety incident, the following external agencies should be informed:	**Information Commissioner's Office**

The school will monitor the impact of the policy using:

1. Confidence of staff and pupils in using technology safely
2. Logs of reported incidents, filtering changes and security issues
3. Surveys and training of
   - Pupils
   - Parents & Carers
   - Staff & Governors

Scope of the Policy

This policy applies to all users of school IT systems, including staff, pupils, Governors, parents and visitors.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated data protection, behaviour and anti-bullying policies and will, where known, inform parents or carers of incidents of inappropriate e-safety behaviour that takes place either in or out of school.

ROLES AND RESPONSIBILITIES

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

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Data Protection Governor which includes the following responsibilities:

- Termly monitoring of e-safety incident logs and reports (included in the termly DPO Report to FGB)
- Reporting to relevant Governor committees/Full Governing Body meetings

Headteacher and Senior Leadership Team:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to authorised staff.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents (included in “Responding to incidents of misuse”) and relevant Local Authority disciplinary procedures).
- The Headteacher is responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Data Protection Officer.
- Acting as a first point of contact for parents, carers or members of the community, in conjunction with the Data Protection Officer.

Designated Safeguarding Lead:

The Designated Safeguarding Lead (DSL) and the Deputy Designated Safeguarding Lead (DDSL) should be aware of e-safety issues and of the potential for serious child protection or 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

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school's e-safety policy and practices
- they have read, understood and signed the staff acceptable use policy (AUP)
- they report any suspected misuse or problem to the Headteacher, senior leadership team or Data Protection Officer for investigation
- all digital communications with students, parents and carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety 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 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.

Data Protection Officer:

The Data Protection Officer is responsible for:

- Producing e-safety/IT security incident logs and reports;
- The production, review and monitoring of the school e-safety policy/documents;
- Reporting regularly to the Senior Leadership Team and the Governing Body
- Providing training and advice for staff and Governors
- Providing data protection and e-safety advice for parents
- Creating and managing a log of incidents to inform future e-safety developments,
- Ensuring the e-safety curriculum is in place and relevant to current technologies and risks;
- Attending relevant Governor committee meetings as required

Computing Co-ordinator

The Computing Co-ordinator is responsible for:

- Mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- providing e-safety training and advice for pupils, staff and parents as required;
- ensuring the e-safety curriculum is in place and relevant to current technologies and risks;
- informing staff of e-safety curriculum resources

Network Manager:

The Network Manager is responsible for:

- The production, review and monitoring of the school IT security procedures;
- Ensuring that the school's technical infrastructure is secure and not open to misuse or malicious attack
- Ensuring that the school meets e-safety technical requirements and any other e-safety policies or guidance that may apply.
- Ensuring that users may only access the network and devices through a properly enforced password protection policy.
- Ensuring that flexible filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Ensuring that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- Ensuring that the use of the schools network and internet services are regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher for investigation.
- Ensuring that monitoring systems are implemented and updated as agreed in school policies

Pupils:

- are responsible for using the schools digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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 the basic concepts of e-safety, including protecting their passwords and personal details, how to use digital devices safely and have a basic understanding of some of the risks associated with using digital technology.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school

Parents and Carers:

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, Parentmail communications, the school website e-safety section and information about national or local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-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
- The sharing of links and online files or data as provided by the school

Community and Visitor Users:

Community users and visitors to the school will usually be assigned either the **Visitor** or **guest.student** login which allows access to the filtered internet service and to locally installed programs and very limited access to server storage.

If community Users and visitors (who are not employed by Hampshire County Council or one of our support companies) require access to any of the school systems as part of a wider school provision will be expected to sign a Community and Visitor User Acceptable Use Agreement before being provided with access to school systems. A copy of the school's Community and Visitor User AUA is included in the appendices.

Parents and volunteers helping with the Library System will need to sign the Staff and Volunteers IT and Internet Acceptable Use Agreement and will use the **Library.change** login, which has restricted access to the school network similar to the **Visitor** or **guest.student** logins.

POLICY STATEMENTS

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing and other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme including assemblies and other relevant activities
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- in lessons where internet use is pre-planned, it is best practice that 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.
- Where Pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents and Carers:

Some parents and carers have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and Parentmail
- The e-safety section on the school's web site, including links to websites etc
- Parents evenings and/or drop in sessions
- Events and campaigns, such as Safer Internet Day

Education – The Wider Community

The school will provide opportunities for local community groups or members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth or voluntary groups to enhance their e-safety provision

Education & Training – Staff and Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- Relevant staff will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This e-Safety policy and its updates will be presented to and discussed in staff meetings or INSET days.
- The Data Protection Officer and Computing Co-ordinator will provide advice, guidance and training to individuals as required.

Training – Governors

All Governors should take part in e-safety training and awareness sessions where possible, particularly those who have a specific responsibility for, or who are members of any committee involved in technology, data protection, e-safety, health and safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant external organisation.
- Participating in school training or information sessions for staff or parents.
- Observing class e-Safety lessons

Technical – Infrastructure, Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- There will be regular reviews and audits of the safety and security of school's technical systems. This information will be kept in the Network Manager's files.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and initial password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password as requested by the Senior Leadership Team.
- The "administrator" passwords for the school system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users by the use of in house Smoothwall filtering. Illegal content (child sexual abuse images) is filtered by Hampshire County Council's filtering provider. Content lists are regularly updated. Staff can request the Network Manager applies changes to the flexible filtering system, but these need prior approval by the Headteacher. The school's filtering is now managed by HantsIT.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the Data Protection Officer.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations will be protected by up to date virus software.
- An agreed process is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed process is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.
- An agreed process is in place that governs the type of executable files programs that staff can install on school devices (home printer drivers, approved alternative browsers, etc)
- The use of removable media (eg memory sticks / CDs / DVDs) by users on school devices is covered in the Bring Your Own Device Policy, but is permissible until remote access becomes available. Personal data cannot be sent over the internet or taken off the school site unless safely secured. Staff are only allowed to use the school email system to send personal data to other staff.

Bring Your Own Device (BYOD)

The school currently permits BYOD for staff and governors to use smartphones and tablets of their choosing at work for their convenience. However, there are a number of IT security and e-safety considerations that need to be met by all BYOD users. Although staff can use their personal mobile phones or other devices for their own use as set out in the Communications section below, this BYOD guidance relates specifically to using personal devices to access school communications, documents and other digital resources relating to the school or its network and is intended to protect the security and integrity of the school's data and technology infrastructure.

The Headteacher reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below. The school will not be responsible in any way for a user's personal device if used for school business. In the event of a technical or data failure the user can approach the Network Manager for advice or help, but this is on the understanding that this support is offered on a goodwill basis and the school or its staff are not obliged to act on this request.

BYOD users are expected to:

- Adhere to the schools policies on e-safety, data protection and safeguarding.
- Use their devices in a responsible way, to ensure that there is no risk to the safety and security of the school systems, devices or other users.
- Install a suitable Anti-virus or Internet Security Suite on their device to ensure infections or other threats are not transferred to the school systems or equipment.
- Ensure the school's personal data is not stored on their device.

- Under no circumstances should photos or videos of pupils be taken or stored on personal devices.

Staff using the Microsoft Exchange or OWA for iPhone/OWA for iPad to access the school's Outlook 365 email system, must digitally agree to allow a remote data wipe of their device when installing or setting up these apps. This function must be used if a device is replaced or lost and the Headteacher should be informed.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use iS not covered by the GDPR/DPA). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents or carers comment on any activities involving other pupils in the images.
- Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of parents or carers.

Communications

This is an area of rapidly developing technologies and uses. A wide range of communications technologies has the potential to enhance learning. The following table shows how the school currently considers these technologies should be used on site:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff supervision	Not allowed
Mobile phones may be brought to school	●							●
Use of mobile phones in lessons				●				●
Use of mobile phones in social time		●						●
Taking photos or videos on mobile phones (not of pupils)			●					●
Use of mobile devices eg tablets, gaming devices			●				●	
Use of personal email addresses in school	●							●
Use of school email for personal emails			●					●
Use of messaging apps		●					●	
Use of social media		●						●
Use of blogs		●						●

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Staff must use the school email service to communicate with others when sharing any type of personal data. However, staff can use personal emails to communicate with each other on the provision that any information transferred does not infringe upon the school's data protection or safeguarding principles.
- Users must immediately report, to the Headteacher or Deputy Head the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any school communication between staff and parents (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Class or group email addresses may be used in specific situations.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only the office@hook-inf.hants.sch.uk email addresses should be used for this purpose.

Inappropriate Activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					●
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					●
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					●
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					●
	Pornography				●	
	promotion of any kind of discrimination				●	
	threatening behaviour, including promotion of physical violence or mental harm				●	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				●	
Using school systems to run a private business					●	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					●	
Infringing copyright					●	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					●	
Creating or propagating computer viruses or other harmful files					●	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					●	
On-line gaming (educational)			●			
On-line gaming (non educational)			●			
On-line gambling					●	
On-line shopping / commerce				●		
File sharing			●			

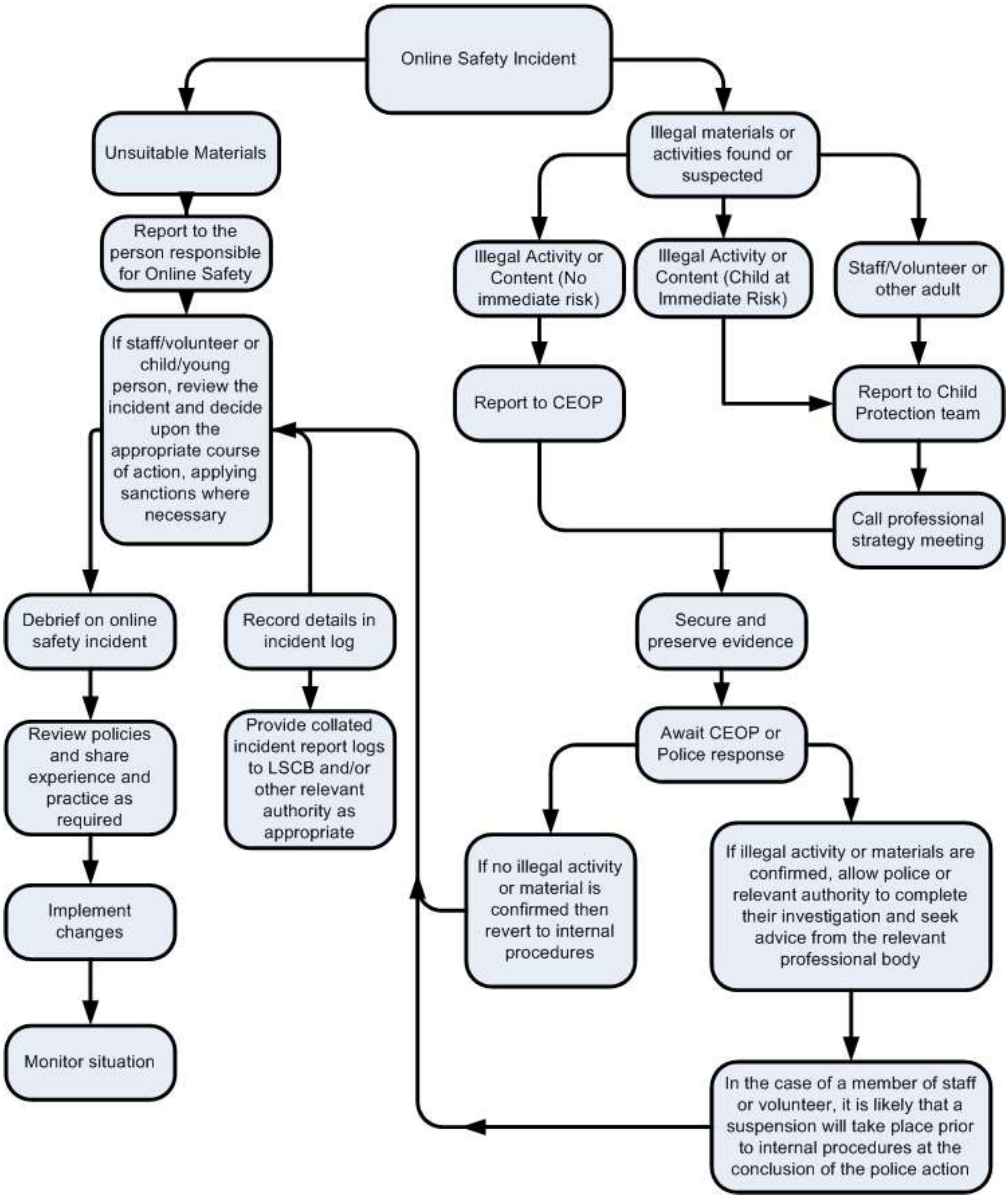
Use of social media				●	
Use of messaging apps				●	
Use of video broadcasting eg Youtube			●		

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Incident Flowchart

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart below for responding to online safety incidents and report immediately to 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

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or other organisations as relevant.
  - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of ‘grooming’ behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour or disciplinary procedures as follows:

Staff Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Network Manager for action re filtering, account change etc	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		●	●	●	●		●
Inappropriate personal use of the internet, social media, personal email, etc	●	●			●		
Unauthorised downloading or uploading of files	●	●			●		
Allowing unauthorised users to access school network by sharing username and passwords or attempting to access or accessing the school network using another person's account without consent	●	●			●		
Careless use of personal data eg holding or transferring data in an insecure manner	●	●					
Deliberate actions to breach data protection or network security rules		●			●	●	●
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		●			●	●	●
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		●				●	●
Using personal email, social networking, instant messaging, text messaging to carry out digital communications with pupils		●					
Actions which could compromise the staff member's professional standing	●	●					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	●	●				●	
Using proxy sites or other means to subvert the school's filtering system		●			●		
Accidentally accessing offensive or pornographic material and failing to report the incident	●	●			●		
Deliberately accessing or trying to access offensive or pornographic material	●	●			●	●	
Breaching copyright or licensing regulations	●	●					
Continued infringements of the above, following previous warnings or sanctions		●	●				●

Pupils Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to Network Manager for action re filtering, account change etc.	Inform parents or carers
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on inappropriate activities).	●	●	●	●	●
Unauthorised use of non-educational sites during lessons	●			●	
Unauthorised use of mobile phone, digital camera, other device	●	●			●
Unauthorised use of social media, messaging apps, personal email, etc	●	●		●	●
Unauthorised downloading or uploading of files	●			●	
Accidentally accessing offensive or pornographic material and failing to report the incident	●	●		●	●
Deliberately accessing or trying to access offensive or pornographic material	●	●		●	●
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	●	●		●	●

Approved by the Governing Body, Hook Infant School

Reviewed and revised: September 2021

Signed ....
Chairman of Governing Body

Date for next review: Autumn Term 2024