Hook Infant School

Online Safety Policy

2024-2027

Contents

Development, Monitoring and Review of this Policy

This Online Safety Policy has been developed by the following staff:

- The Headteacher
- Deputy Head
- Computing Lead
- PSHE Lead
- Data Protection Officer

Consultation within the school community takes place through Parentmail communication, online surveys, and an 'open door' policy for parents and community.

Schedule for Development, Monitoring and Review

This Online Safety Policy was approved by the Governing body on:	**See Page 10**
The implementation of this Online Safety Policy will be monitored by the:	**Digital Lead with the aid of the PSHE & Computing Leads & DPO**
Monitoring will take place at regular intervals:	**Annually or as required**
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	**Autumn Term 2027**
Should serious online safety incidents take place, the following external agencies should be informed:	**LA Safeguarding Officer Police/SEROCU www.ceop.police.uk**
Should any data breaches occur as a result of an online 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 online 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 online safety behaviour that takes place either in or out of school.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports in the termly Data & IT Security Report produced by the school's DPO. A member of the Governing Body has taken on the role of Data Protection Governor which includes the following responsibilities:

- Termly monitoring of Data & IT security incidents 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 online safety) of members of the school community, though the day to day responsibility for online 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 online safety allegation being made against a member of staff. (see flow chart on dealing with online 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 online 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 online 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.
- The Headteacher will act 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 Leads (DDSL) should be aware of online 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 online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Digital Lead

The Digital Lead is responsible for:

- strategic oversight of all digital technology and associated areas and how these integrate with the school's development plan
- creating and managing the school's Digital Technology Strategy
- ensuring digital technology and associated procedures and initiatives are embedded across the school

PSHE & Computing Leads

The PSHE and Computing Leads are responsible for:

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

Data Protection Officer

The Data Protection Officer is responsible for:

- producing Data & IT security incident logs and reports
- the creation, review and monitoring of the policies and procedures relating to Data & IT Security
- reporting regularly to the Senior Leadership Team and the Governing Body
- providing training and advice for staff and Governors
- providing data protection and IT security advice for parents
- attending relevant Governor committee meetings as required

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 online safety technical requirements and any other relevant 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 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 data & IT technical information in order to effectively carry out their 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

Teaching and Support Staff

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's online 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
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online 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

Pupils

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 online 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 online 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 online safety section and information about national or local online safety campaigns. 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
- 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, but 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 an Acceptable Use Policy (AUP) before being provided with access to school systems.

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 online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety will be a focus in all areas of the curriculum and staff will reinforce online safety messages across the curriculum. The online safety curriculum will be broad, relevant and provide progression, with opportunities for creative activities.

- a planned online safety curriculum will be provided as part of PSHE, Computing and other lessons and will be regularly revisited
- key online safety messages will be reinforced as part of a planned programme including assemblies and other relevant activities
- pupils swill be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information
- pupils will 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 will act as good role models in their use of digital technologies, the internet and mobile devices
- 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 online 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 online 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 online 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 online safety knowledge and experience. This may be offered through:

- online safety messages targeted towards grandparents and other relatives as well as parents
- providing online safety information for the wider community through the school website
- supporting community groups e.g. Early Years Settings, Childminders, youth or voluntary groups to enhance their online safety provision

Education & Training – Staff and Volunteers

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

- a planned programme of formal online safety training that is available to staff. This will be regularly updated and reinforced
- all new staff receiving online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements

- relevant staff will receiving regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- this online safety policy and its updates being presented to and discussed in staff meetings or INSET days
- the Digital Lead, PSHE & Computing leads and the DPO providing advice, guidance and training to individuals as required

Training – Governors

All Governors will take part in online 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, online safety, health and safety and child protection. This may be offered in a number of ways including:

- 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 online 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 online 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 Fortigate filtering and monitoring. Content lists are regularly updated and staff can request the Network Manager applies changes to the filtering system, but these need prior approval by the Headteacher. The school's filtering is currently managed by Agile ICT
- 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" (e.g. 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 (e.g. memory sticks / CDs / DVDs) by users on school devices is not permitted without prior approval by SLT, but all staff have access to 50GB storage as part of their Microsoft 360 account. Teaching and admin staff have the use of secure remote access to school systems. 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
- A personal mobile device policy has been created for staff and school visitors. Pupil use of personal mobile devices is covered below

Use of Personal Mobile Devices

Staff and visitors
The school currently permits staff and governors to use smartphones, tablets and other mobile devices at work for their convenience. Other visitors (such as contractors or volunteers) will also bring their personal mobile devices into school. However, there are a number of IT security and online safety considerations that need to be met by all personal mobile device users. The separate policy, "**Personal Mobile Device Policy for Staff and Visitors**" outlines the restrictions for staff, governors and other visitors and is intended to protect the security and integrity of the school's data and technology infrastructure, while meeting safeguarding obligations.

Pupils
To ensure a safe, focused and distraction-free learning environment for all pupils, the use of personal mobile devices, including but not limited to mobile phones and smartwatches, is strictly prohibited on school property. Mobile devices can disrupt lessons, hinder social interactions, and pose potential risks to privacy and security. By restricting their use, Hook Infant School aims to foster better concentration, avoid conflict or issues arising from lost, stolen or broken devices and protect the well-being of all pupils within school. Parents are encouraged to support this policy by ensuring their children leave personal mobile devices at home or hand them over to school staff upon arrival, for collection at the end of the day. If a pupil is found in the possession of a personal mobile devices, these will be held in the school office and will be released to the parent or carer at the end of the school day.

Communications

This is an area of rapidly developing technologies and uses. A wide range of communications technologies have the potential to enhance learning. When using communication technologies on site the school considers the following as good practice:

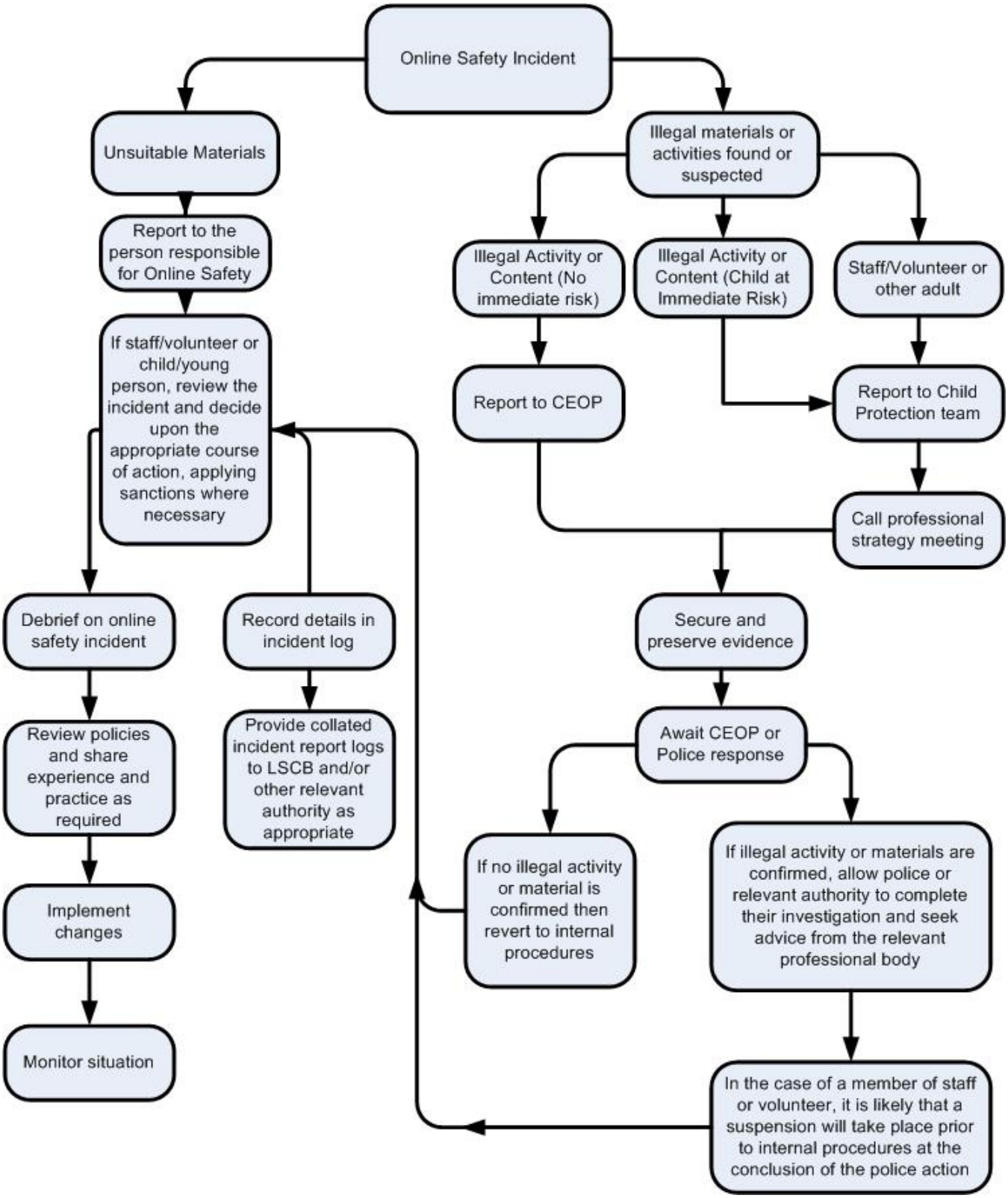
- the official school email service may be regarded as safe and secure. Staff must use the school email service to communicate with others when sharing any type of personal data. However, staff can use personal emails or other messaging tools (such as WhatsApp) to communicate with each other on the provision that any information transferred does not infringe upon the school's data protection or safeguarding principles
- when sending personal data via email, staff must always use a ***CONFIDENTIAL*** tag at the beginning of the subject line. This will flag to recipients that they must only open the email after normal teaching hours and/or when they cannot be overlooked by staff, unauthorised persons or pupils.
- 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 will be taught about online 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

Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities e.g. cyber-bullying is banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but are 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.

Incident Flowchart

If there is any suspicion that the website 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.



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:

- more than one senior member of staff will be involved in this process. This is vital to protect individuals if accusations are subsequently reported
- the procedure will be conducted 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. The same computer will be used for the duration of the procedure
- ensure that the relevant staff 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 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.

Approved by the Governing Body, Hook Infant School

Reviewed and revised: September 2024

Signed Alison Collier

Chairman of Governing Body

Date for next review: Autumn Term 2027