



Name of school:	Hiltingbury Infant School
Name of Responsible Headteacher:	Mrs Phillippa Longman
Date approved by Governing Body:	24.1.23
Date of review by Governing Body:	January 2024

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.

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher 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, appendix 1 – “Responding to incidents of misuse”)
- The Headteacher is responsible for ensuring that teaching staff receive relevant online safety training.

Network Manager/Technical Staff

Those with technical responsibilities are responsible for ensuring:

- 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 Hampshire online safety policy/guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy

Teaching and Support Staff

Are responsible for insuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices.

- They have read, understood and signed the staff acceptable use policy/agreement.
- They report any suspected misuse or problem to the Headteacher for investigation/action/sanction.
- All digital communications with students/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,
- Pupils understand and follow the online safety rules, according to the acceptable use policy.
- In lessons where internet use is pre-planned, pupils will be guided to sites that have been checked as suitable for their use.

Pupils

Pupils are responsible for using the schools digital technology systems in accordance with the 'Computing and Online safety rules'.

Parents/Carers

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

- Digital and video images taken at school events
- Access to parents' sections on the website

Policy Statements

Education – Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways. A planned online safety curriculum will be provided as part of Computing/PSHE lessons and will be regularly revisited.

- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Key online safety messages will be outlined in the 'Computing and Online Safety' rules poster, see Appendix 2

- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating issues and helping them to understand how they can influence and participate in decision-making.

Education – Parents/Carers

Many parents and carers have only 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/regulation of the children's online behaviours. Hiltingbury Infant School will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. safer internet day
- Reference to the relevant web sites/publications e.g. www.swgfl.org.uk
www.saferinternet.org.uk

Education and Training – Staff/Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.

Training – Governors

Governors should take part in online safety training/awareness sessions.

Technical – infrastructure/equipment, filtering and monitoring

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- 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 secure password. Users are responsible for the security of their username and password
- Internet access is filtered for all users.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile technologies (including iPads, laptops and chromebooks)

- The school acceptable use agreements for staff and parents/carers will give consideration to the use of mobile technologies.
- The school allows:

	School devices		Personal devices		
	Single user	Multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	✓	✓	X	✓	✓
Full network access	✓	✓			
Internet only					✓
No network access			X	X	X

Aspects that the school may wish to consider and be included in their online safety policy, mobile technologies policy or acceptable use agreements:

School owned devices:

- Desktops to be used in classes, PPA room and pods by teaching and support staff. IPADs to be used by all staff and children from allocated trolleys. Class teacher IPADs to be used by staff only.
- No personal use is allowed of school equipment
- Our IT technical support and computing lead will Manage devices/installation of apps/changing of settings and the Headteacher alongside these staff monitor
- We have one afternoon a week of Technical support who comes on site to manage the IT across the school.
- All access is filtered through the internet provider settings in partnership with the schools IT support.
- Access to cloud services will be via office 365 login sharepoint.
- This will comply with the Data Protection policy
- Images must only be taken on school devices with gained consent and must not be kept once the child/staff has left the school.

- Staff training within induction to all IT equipment including passwords, email access.

Personal Devices

- Staff and visitors are able to use personal mobile devices in school following our code of conduct policies and procedures, they must NOT be used when with children
- Personal devices to only be used when away from children and where possible in the staffroom.
- These must be stored in a cupboard or the staffroom
- Staff will be allowed to use personal devices for school business e.g. emails, report writing, CPOMS. Code of conduct must be used and no information to be saved onto personal devices, password protected memory sticks must be used to save anything.
- All visitors will have no access to the school network. Some approved visitors e.g. HIAS/Ofsted will be given internet access where necessary.
- No technical support available
- Filtering of the internet connection to these devices
- This will comply with the Data Protection policy
- It is forbidden to Take/store or use images on personal devices
- Visitors will be informed about school requirements on entry by school office staff
- The safe and responsible use of mobile devices is embedded in the school online safety education programmes with the support of our cyber ambassadors.

Use of digital and video images

The development of digital image 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. Such images may provide avenues for online-bullying to take place. The school will inform and educate users about potential risks associated with this 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 e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation (GDPR 2018).

The school will ensure that:

- It has a Data Protection Policy.

- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- It will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- It provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice)
- Procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.

- It [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media (including USB's) the:

- Data must be encrypted and password protected
- Device must be password protected
- Device must be protected by up to date virus and malware checking software
- Data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times, take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Will not transfer any school personal data to personal devices except as in line with the school policy
- Access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data

Communications

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

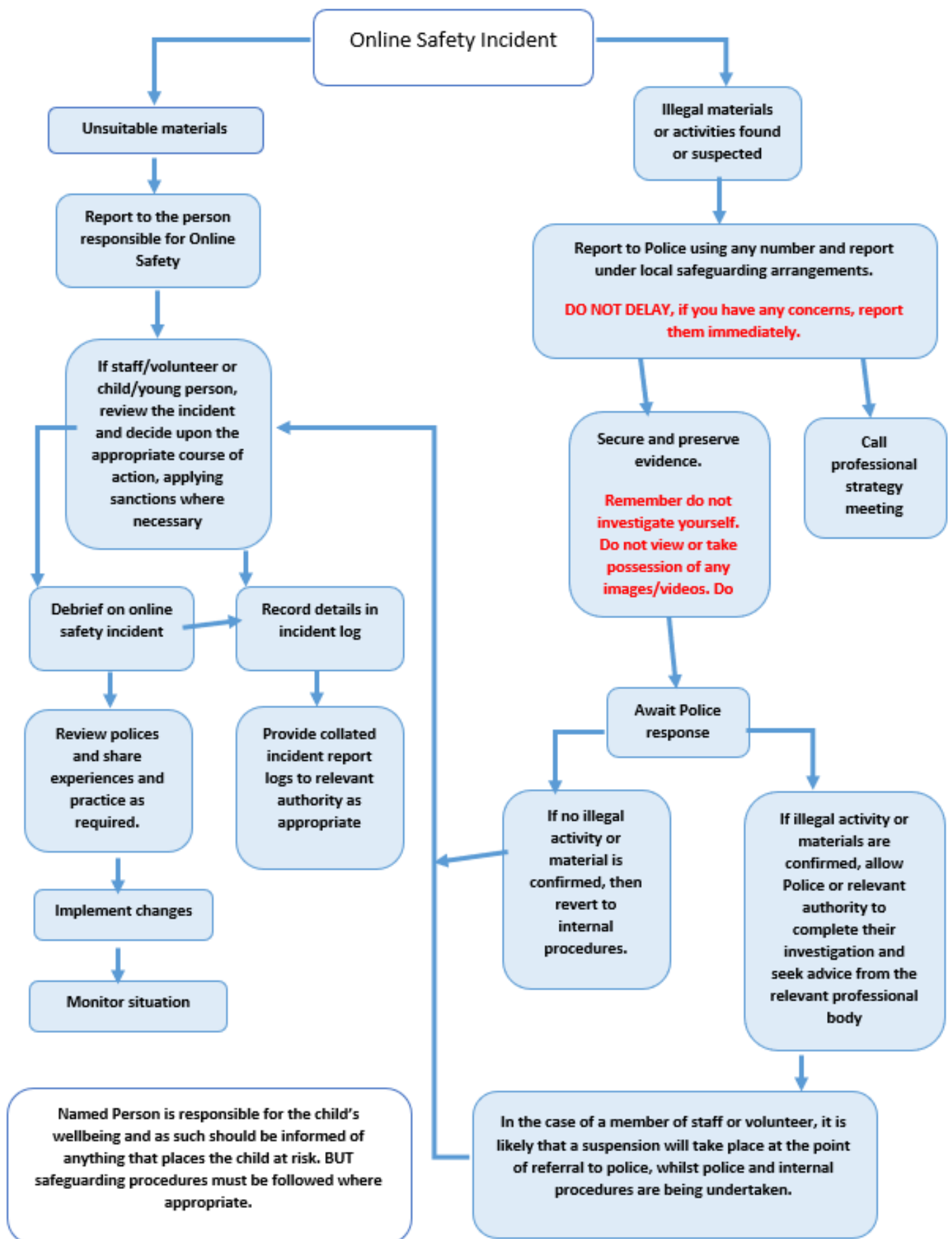
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents/carers must be professional in tone and content.

Illegal Incidents

If there is any suspicion that the web site concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (Appendix 1) for responding to online safety incidents and report immediately to the police.








Appendix 1





Computing and Online Safety Rules

This is how we stay safe when we use computers and tablets:

	I will ask a trusted adult if I want to use the computers/tablets.
	I will only use activities that a trusted adult has told or allowed me to use.
	I will take care of computers/tablets and other equipment.
	I will ask for help from a trusted adult if I am not sure what to do, or if I think I have done something wrong.
	I will tell a trusted adult if I see something that upsets me on the screen.
	I will always keep my passwords safe.
	I will not share personal information about myself online (name, address, age).