THE FEDERATION OF BURLEY AND SOPLEY PRIMARY SCHOOLS

Online Safety Policy

Date of issue	Autumn ‘23	**Date to be revised**	Autumn ‘24

Names of relevant post holders

Post	**Holder**	**Post**	**Holder**
Headteacher	Nanette Allies	**Chair of Governors**	Ian Satchwell
SENDCo/Inclusion Lead	Claire Bleakley	**Data Protection Officer**	Clare Roche
Online Safety Lead	Nanette Allies	**Online Safety Governor**	Stewart Robinson

Revision Log (last 5 changes)

Date	**Version No**	**Brief details of change**
18/09/2023	1	Policy created using Hants model policy
20/10/2023	2	Introduction added below - taken from our Child Protection Policy. Roles within the school added - Online Safety Group

Introduction

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes’.

- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group (https://apwg.org/).

We ensure that online safety is a running and interrelated theme when devising and implementing policies and procedures.

Roles within our schools

The Federation of Burley and Sopley Primary Schools has an Online Safety Group which consists of the headteacher (online safety lead), the DSL's (safeguarding), the lead teacher for the IT curriculum, the link governor and policy and technical staff.

The Online Safety Group have undertaken role specific training and fully understand their roles within the schools.

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 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 ensuring 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 and understood the Acceptable Use Policy Acceptable Use of IT Policy Autumn '23
- they report any suspected misuse or problem to the Headteacher for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems

Designated Safeguarding Lead/Deputy Designated Safeguarding Leads

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues that can arise.

Students/Pupils:

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement

Education

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 should be provided as part of Computing/PSHE/other lessons and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students/pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Education & Training – Staff/Volunteers

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 is in place for the Online Safety Group. This will be regularly updated and reinforced.
- Regular reminders are emailed to all staff with the latest updates in online safety and risk.
- An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should fully understand the school online safety policy and acceptable use agreements.

Training – Governors/Directors

The link governor should receive online safety training.

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

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

Use of digital and video images

- When using digital images, staff should inform and educate students/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

The school must ensure that:

- It has a Data Protection Policy. 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 to the 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 Privacy Notice - Pupils and Parents (GDPR)
- 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 72 hrs 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 school is 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 the:

- Data must be encrypted and password protected.
- Devices 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 once it has been transferred or its use is complete.

St**aff must ensure that:**

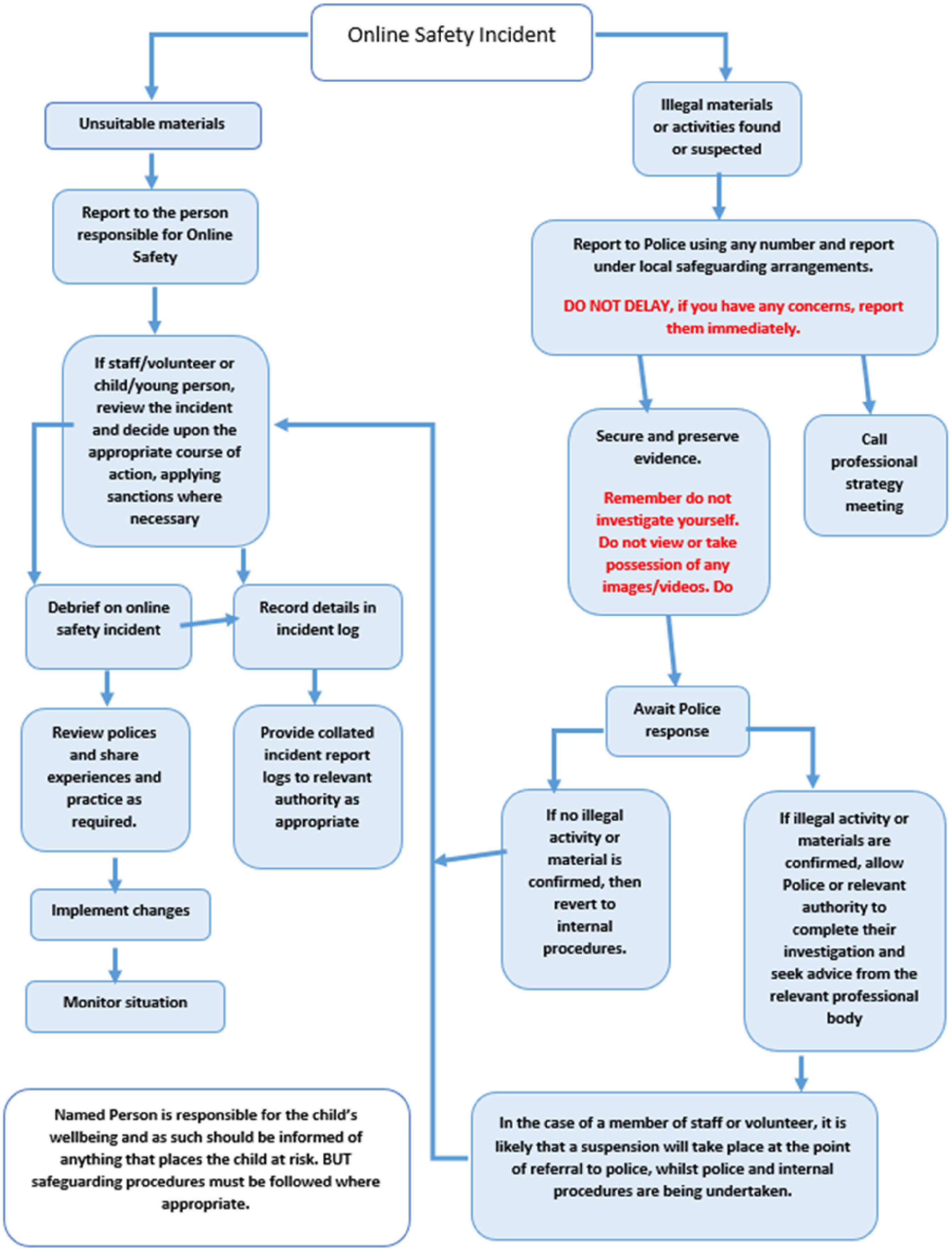
- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- They can help data subjects understand their rights and know how to handle a request whether verbal or written and 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.
- They will not transfer any school personal data to personal devices except as in line with school policy
- They 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:

- 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 a 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

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await 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 at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.