Hedon Primary School
E-safety Policy

Approved by committee 27th October 2020
Approved by full governors 3rd November 2020
Reviewed 13th Oct 2022

Writing and reviewing the e-safety policy
This policy has been developed to ensure that all stakeholders at Hedon Primary School work to ensure safeguarding and promotes the welfare of children and young people. We aim to put effective management systems in place to maximise the education and social benefits obtained from ICT use whilst minimising the risks. This policy relates to other policies including those for ICT, Acceptable Use, Behaviour and for Child Protection.

Teaching and learning
Internet Access

- The Internet is an essential element in 21st century life for education, business, and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Our internet provision will be filtered using the Local Authority mediated filtering system.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and use will enhance learning
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience.
- Pupils will be taught how to evaluate Internet content and the school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report inappropriate and unpleasant Internet content.

Pupil email use
Pupils are provided with an @hedonprimaryschool email address which is used from EYFS to log pupil's into chromebooks and their online accounts such as, but not limited to Google Classroom, TTRockstars and Spelling Shed. Wonde QR codes (magic badges) are used to sign in rather than younger pupils needing to remember lengthy emails and passwords.
When pupils begin using the email facility, they read, discuss, and sign the following agreement:
I have been provided with a @hedonprimaryschool.co.uk email address. I agreed that:
● this email address will only be used for school purposes
● that I will only log in when asked by a teacher
● I know that I cannot send emails to anyone outside of our domain @hedonprimaryschool.co.uk
● I will not use the email address to register for an online account unless asked by a teacher (such as Scratch and other sites already used in school)
● I know that my email address will be deleted if I misuse it in any way or do not follow the above agreement.

Published content and the school website / social media accounts

- Staff or pupil personal contact information will not be published. The contact details given online must be the school office; parents are also notified that they can contact the teacher via the class Seesaw account.
- The headteacher will take over all editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified.
- Pupils' names will not be used in association with photographs anywhere on the school website or other sites for example Seesaw, Facebook, or Twitter.
- Pupils' names will not be used in association with photographs anywhere on the school website or other site for example, Facebook or Twitter. Seesaw is different in that it is a closed group - only approved parents/carers have access to it and, if photograph permission has been received, photographs will be linked to individuals, groups or the whole class and as such pupils may be identifiable.

- Pictures and work will only be shown on the website if parents/carers have signed the consent form issued at the start of their school life. This permission can be altered or withdrawn at any time by parents.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Managing videoconferencing & webcam use

- When available, Skype, video conferencing and webcam use will be appropriately supervised for the pupils' age. Video conferencing equipment will always be shut off when not in use.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Social media platforms and online gaming are becoming a bigger part of life and increasingly used by pupils outside of school, often of an age below that recommended by the site. While we do not wish to dictate to parents what their child should, or should not, be doing at home, we have to accept that it is happening and must adapt teaching and support as the need arises.
    - The SLT will share relevant and appropriate ESafety messages with parents
    - Teachers will include discussions in Computing & PSHE about the use of social media, safety messages and mental health. While the impact of social media and online gaming on mental health is yet to be scientifically confirmed, as a school we witness the impact on behaviour and mental health (e.g. social/emotional needs).

Protecting personal data

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998.
- In line with the Acceptable Use Policy, data will only be stored on the cloud-based storage provided by the school.
- Logins and passwords must be kept private and not shared.
- Computers will be locked when not in use. (Ctrl + Alt + Del) if available.

Procedures

- The school ICT system's security will be reviewed regularly.
- Virus protection will be updated regularly.
- Acceptable use posters will be displayed around the school.
- The school will work in partnership with parents, the LA, DES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, which aren't blocked, the URL (address) and content must be reported to the Local Authority via the Head, ICT co-ordinator and the E-Safety Coordinator informed (Reporting questions and Protocol Appendix 1,2,3).
- If a pupil or member of staff finds that a website that is blocked by any filtering, they need to complete a report. The link to the online form is listed as a useful site and easily available on every staff device.
- Pupils will be regularly reminded to inform their teacher when a website has been blocked. The IT coordinator receives a notification every time and this can be cross checked with the teacher's reports.
- Where reports are not provided by staff, this will be followed up by the IT coordinator.
- The IT coordinator will analyse the reports from the staff form as well as Securely / Smoothwall reports to identify patterns in behaviour, trends, vulnerabilities and specific pupils in need of additional ESafety work/ELSA, which will then inform future IT planning, equipment uses and filtering settings.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.
- E-Safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.

- E-Safety briefings and materials will be made available to parents.
- Pupils will be taught how to block someone online or report them using the CEOP button.
- Discretion and professional conduct are essential.
- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging, or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.
- Cyber-bullying will be dealt with using the school's behaviour protocols and is seen as a serious offence.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with School child protection procedures and logged on CPOMS.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

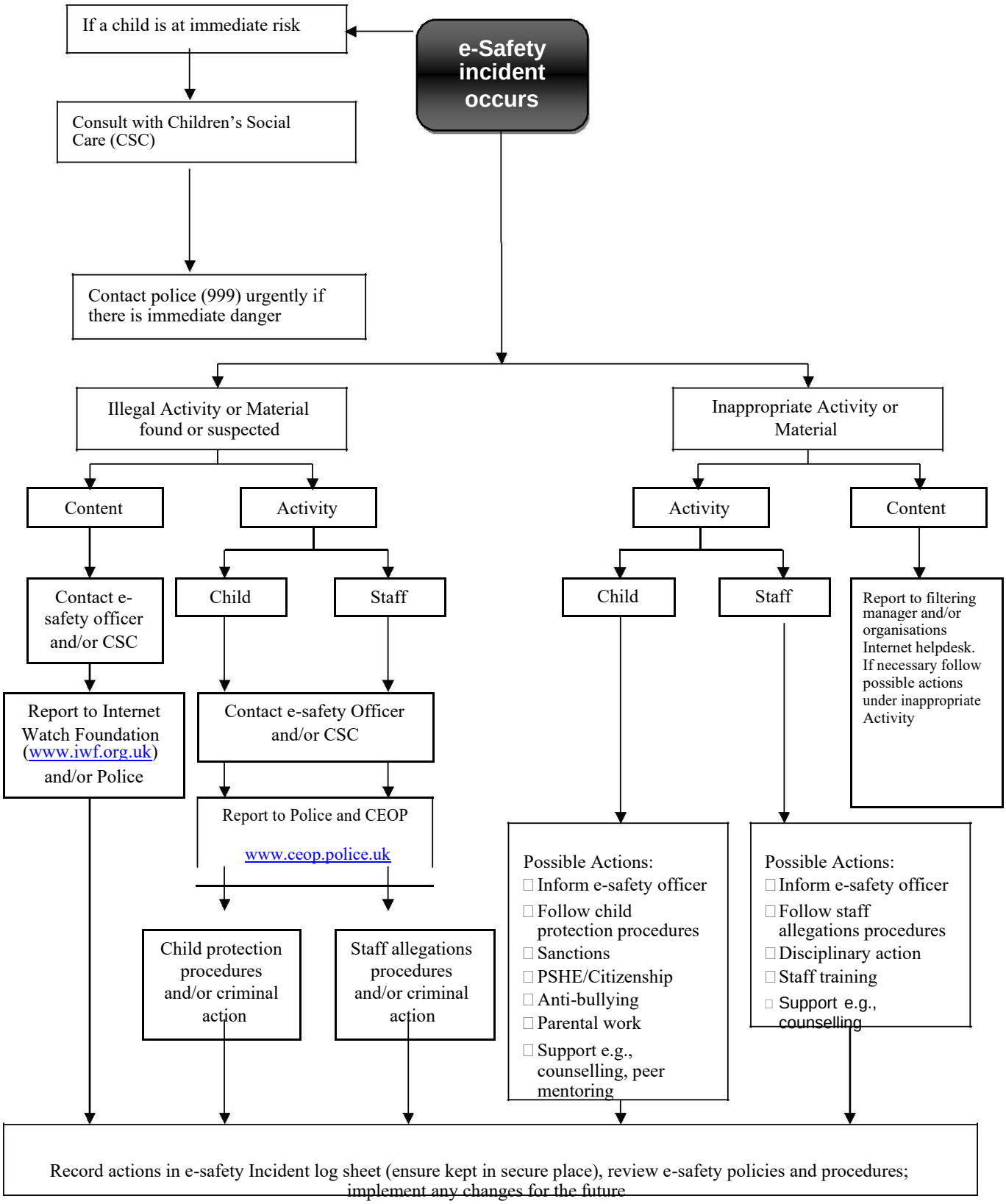
Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website.
- The school will ask all pupils and staff to sign the relevant agreements at the start of each key stage, or when children are admitted in the case of in-year admissions.

Google Form questions:
1. Date of incident
2. Time of incident
3. Name of pupil involved
4. Name of staff making report
5. What type of device was being used?
6. Details of incident - e.g. which lesson did it happen in, what the child was using the device for, did a particular search bring about the blocked website (what were they actually searching for?)
7. Do you need me to follow this up with the child? e.g. it was a deliberate action and they need ESafety / ELSA support.
8. Where was the child sitting?
9. Please tell the child they have done the right thing by telling you. Unless you know they were deliberately searching for something inappropriate, remind them they are not in trouble and that the filter caught something they don't need to see.
10. Do you need to tell you more about any of the above questions or tell you something more.

Log sheet 1 is replaced by Google form (questions listed above) and log sheet 2 has been replaced by CPOMS - I think we can remove them from this policy but state that any deliberate pupil e safety incidents or breaches of filtering should be reported initially to us, then logged in CPOMS.

HEDON PRIMARY SCHOOL



HEDON PRIMARY SCHOOL – Use if online form can't be used.

e-Incident Log Sheet 1 – "member of staff identifying incident" – front cover

To be completed by the member of staff identifying the incident					
Date of identification:		Date of incident (if different):			
Time of identification:		Time of incident (if different):			
Duration of incident:		Do you know if repeat victim?	yes	no	unsure

Description of the e-Safety incident:
(please give as much information as you are able – use the prompts overleaf in the guidance)

Description of information recorded or secured **(please refer to legal guidance overleaf)** Have files, audio/text/images been recorded and secured? Has any computer or other technology including phones been secured?	Yes	No

If yes, how and where, who by and when?

What actions were taken, and by whom? *Give details of agencies informed and contact person within those agencies.*

Name of person completing this form:			
Organisation:			
Date:		Signature:	

Send this form immediately to the person with responsibility for child protection within your organisation

Date and Time section:
Please complete all sections, if you don't know the exact day or time of the incident, please write 'unknown'

Description of the e-safety incident:
It is vital that all details you know are recorded, including how the information became known to you and from whom. If there is insufficient space on the form, please use additional sheets, but ensure that they are firmly attached and a note clearly identifies additional sheets used. Include detail of specific services or websites used if known (e.g., chat room, instant messenger); e-mail addresses; usernames etc. Give full details of real names and e-mail addresses etc where known. Some prompts to assist you could be:
How was the incident identified? Who was involved and how do you know this? Why do you have concerns?

Description of information recorded or secured
Legal guidance for those reporting e–Safety incidents that involve a criminal offence
POWERS
If **any person** has reasonable grounds to believe that an offence IS being committed, then they may **detain the person (offender only)** and **secure any evidence** of the offence (including property). This would include the property of a victim or offender. Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984.

Offences committed via computers/laptops/mobile phones.
In these situations the securing of information **must be carried out in a specific way** in order to obtain the best evidence possible for the police and other law enforcement agencies. When a computer is turned on or on standby it should be **left exactly as it is**; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to **record in note form** any details that can be seen on the screen. **DO NOT follow any links or change any pages**.
Information that should be noted if on screen:

- Website address.
- Email addresses of sender and recipient.
- Dates and Times.
- User names.
- Mobile phone numbers.
- Any profile information.
- Any text from chat conversations.

If a request for inappropriate behaviour is made on MSN, FACEBOOK, any chat forum or social networking site. **DO NOT DELETE or interfere with the offending account**, (this will be done when the evidence is secured). This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners.
The above information is not an exhaustive list and any other information noted on screen should be included.

Actions taken
Please give full details of other agencies that have been informed. If the police have not been informed, this must be noted, together with reasons, as e-safety incidents extend well beyond 'grooming' and may be linked to other criminal activity. This may include racist incidents, radicalisation or bullying online, please see legal framework section 4.2 for a comprehensive list. The form must then be signed and dated and handed as soon as possible to the person responsible for child protection within your organisation

HEDON PRIMARY SCHOOL

e-Incident Log Sheet 2 – "Notifications and Actions" – person with responsibility for child protection

To be completed by the person with responsibility for child protection within the organisation		
Notifications: 1. Was notification to the Local Authority Designated Officer required? 2. If yes, what was the outcome? 3. Have you notified the police? 4. Please give details with **reference to guidance overleaf**. **NB This is not an exhaustive list there may be other actions you are required to carry out within your specific organisation.**	Yes	No

Conclusion to the incident:		
Have specific vulnerabilities or trends been identified?	Yes	No
If yes, what action will now be taken?		

Name of person completing this form:			
Organisation:			
Date:		Signature:	

Notifications

Please give full details of other agencies that have been informed. The person initially identifying the incident may have already contacted others, please also record them here, plus any additional action taken by you after receiving the completed Log Sheet 1.

As with Log Sheet 1, if the police have not been informed, this must be noted, together with reasons, as safety incidents extend well beyond 'grooming' and may be linked to other criminal activity. This may include racist incidents, radicalisation or bullying online, please see legal framework section 4.2 for a comprehensive list.

It is possible that information has not been recorded and secured by the member of staff completing Log Sheet 1. You are reminded that you have powers to detain and secure if you have reasonable grounds to believe that an offence IS being committed.

You may **detain the person (offender only)** and **secure any evidence** of the offence (including property). This would include the property of a victim or offender.
Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984.

Offences committed via computers/laptops/mobile phones.
In these situations the securing of information **must be carried out in a specific way** in order to obtain the best evidence possible for the police and other law enforcement agencies.
When a computer is turned on or on standby it should be **left exactly as it is**; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to **record in note form** any details that can be seen on the screen. **DO NOT follow any links or change any pages**.
Information that should be noted if on screen:

- Website address.
- Email addresses of sender and recipient.
- Dates and Times.
- User names.
- Mobile phone numbers.
- Any profile information
- Any text from chat conversations.

If a request for inappropriate behaviour is made on MSN, FACEBOOK, any chat forum or Social networking site. **DO NOT DELETE or interfere with the offending account**, (this will be done when the evidence is secured). This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners. The above information is not an exhaustive list and any other information noted on screen should be included.

Conclusion to the incident

Please record any disciplinary action taken or communications with parents or carers, as well as specific detail of future meetings, monitoring or discussion planned.

Vulnerabilities and Trends

If there are additional vulnerabilities and trends that have been revealed by the incident, there may be a need to review organisational policy or pass information to other agencies later, either once the investigation has been concluded or even before that. Please record all details that you are able to provide at this stage.