Sun Hill Junior School

ICT, Computing & E-safety policy

Name of School	Sun Hill Junior School
Date of Policy Issue/Review	November 2025/November 2026
Name of Responsible Manager/Headteacher	Sue Griffiths (HT & DSL)
Chair of Governors	Michelle Andrews
Date approved by Governors if statutory:	Non-statutory

1. Introduction

Technology offers enormous educational, social and creative benefits and is integral to the lives of our pupils, both in school and beyond. At Sun Hill Junior School we aim to equip our pupils with the skills, confidence and knowledge they need to navigate the digital world safely and responsibly. We will embed safe, responsible and positive online behaviours throughout the curriculum, our culture, and our use of digital systems and devices.

We believe that online safety is not simply about *protection from harm*, but also about *empowering children* to make informed, positive choices online — promoting digital resilience, creativity and opportunity, while managing risks.

This policy sets out the systems, practices, responsibilities and culture we will maintain to embed safe and responsible use of technology across the school. It should be read alongside our policies on:

- Child Protection / Safeguarding
- Acceptable Use (Staff / Volunteer and Pupil)
- Staff Conduct
- GDPR / Data Protection

2. Aims

We aim to:

- Raise children's awareness of the importance, power and potential,both positive and negative, of technology in the world today.
- Teach children how to use, understand and apply a wide range of technology to enhance and improve their work across the curriculum.
- Empower children's attitudes towards technology and support them to recognise their responsibilities when engaging with digital tools and online environments, both in school and in their personal lives.
- Provide a safe, resilient, and inclusive digital learning environment where pupils, staff, volunteers and families understand risks and opportunities and are supported to use technology positively.
- Ensure our filtering, monitoring, safeguarding and data-protection measures align with current national guidance, and that all users understand their role in maintaining them.

3. Scope

This policy applies to:

- All pupils, staff, governors, volunteers, contractors and visitors who use the school's ICT systems, devices or network (on-site or off-site).
- All school-provided devices (e.g., laptops, Chromebooks, tablets, interactive whiteboards) and peripherals.
- Personal devices when used for school business or when connected to the school's network or systems (including remote access).
- All online activities undertaken using school systems or devices, or personal devices in a school/educational context.
- All users' online behaviour where it affects the school, other members of the school community, the school's reputation or the safety of individuals.

4. Curriculum & Teaching

4.1 Curriculum

- Computing lessons meet the requirements of the National Curriculum programmes of study and are differentiated where appropriate for pupils.
- We use recognised frameworks (the Education for a Connected World framework and the DfE guidance on Teaching Online Safety in Schools) to support planned progression in online-safety knowledge and skills.
- Pupils learn to:

  - Use technology safely, respectfully and responsibly.
  - Recognise how technology can affect self-image, relationships, reputation, health and wellbeing, privacy and security.
  - Understand how digital systems work and how to apply these safely.
  - Use digital tools to express themselves creatively, collaborate, explore and solve problems.
  - Respond appropriately to new and evolving technologies, including generative AI, ensuring safe and critical use. (Note: updated filtering/monitoring standards require awareness of risks from AI tools.)
- We also embed online safety education within other curriculum areas (e.g., PSHE/RSHE, assemblies, circle-time) and link it across our wider curriculum to promote a "whole-school" approach.

4.2 Teaching & Learning

- Teaching will be active, relevant and practical, enabling children to use technology safely and meaningfully for learning, collaborating, exploring and communicating.
- We recognise children will arrive with a wide range of prior experience of technology and will plan accordingly, with progression in skills, deeper challenge, and opportunities to use a variety of devices and tools.
- Access to hardware and software (e.g., Chromebooks, laptops, tablets) will support learning. We aim to ensure equitable access for all pupils, including those with SEND, those from disadvantaged backgrounds and those with limited home access.
- We will ensure that any online learning, remote education or homework uses safe platforms, is supervised appropriately and links to this online-safety policy.

5. Education for Safe & Positive Online Behaviour

5.1 Pupil Education

- At the start of each academic year (and throughout each term), pupils will be taught online-safety lessons and reminded of our acceptable-use rules.
- We promote positive online behaviours: safe interaction, respectful communication, digital citizenship, understanding impact of actions, recognising risks.
- We deliver sessions addressing key risks such as online bullying, grooming (though not using this vocabulary), 'fake' news and websites, the need to check facts, sharing inappropriate images, privacy, AI misuse, health/well-being concerns, and digital footprint.
- We involve pupils in peer-support/ ambassador roles (e.g., "Cyber Ambassadors" scheme) to build leadership, awareness and responsibility.
- We use age-appropriate language, resources and pedagogy to ensure understanding and engagement by all pupils, including younger and vulnerable pupils.

5.2 Staff Education & Professional Development

- All staff and volunteers receive induction training in online safety, safeguarding, filtering/monitoring, data protection and their roles/responsibilities.
- Ongoing professional development will maintain currency with emerging risks (e.g., generative AI, new apps, online challenges) and support safe and effective use of technology in teaching.
- Staff are expected to model safe and responsible use of technology (both in and out of school) and follow our Acceptable Use and Staff Behaviour policies in relation to personal and professional digital behaviour.

5.3 Parental/Carer Education & Engagement

- We provide parents/carers with information and guidance to support their child's safe and responsible use of technology at home.
- We communicate our online-safety policy, acceptable-use agreements and expectations in newsletters, the school website and parent briefings.
- We engage parents/carers as partners in promoting positive digital behaviours and reducing risk at home and in the community.

6. Systems, Infrastructure, Filtering & Monitoring

- We will ensure our ICT infrastructure (hardware, network, cloud services, devices) and online-platforms (e.g., Google Classroom) are configured securely and support safe use by pupils and staff.
- Our internet access is filtered and monitored appropriate to pupils' age and risk profile; we ensure compliance with the DfE Filtering & Monitoring Standards.
- We annually review our filtering, monitoring and infrastructure arrangements (or sooner if new devices/technologies are introduced) to ensure it reflects our risk profile (e.g., SEND/EAL pupils) and emerging threats (including generative AI).
- We assign clear roles and responsibilities (SLT, DSL, MAT IT lead, governors) for filtering/monitoring and ensure that staff are aware, trained and understand their responsibilities.
- Monitoring includes both real-time technical monitoring (where appropriate) and human oversight (e.g., classroom supervision, reviewing logs/alerts).
- We recognise that filtering/monitoring is only one part of safeguarding; teaching pupils to assess risk and behave safely is equally important.
- We have robust incident-reporting and response procedures for online-safety concerns (e.g., inappropriate content accessed, online bullying, grooming, radicalisation). These tie into our Child Protection / Safeguarding policy and procedures.

7. Pupil – Acceptable Use & Behaviour

- Each pupil will sign (or have a parent sign) an Acceptable Use Agreement (AUA) appropriate to their age, setting out their responsibilities and our expectations for safe, respectful use of technology.
- Pupils understand that all use of the school network, devices, platforms and internet access is monitored and that they are responsible for their behaviour online.
- Clear rules (age-appropriate) will be communicated, covering:
  - never giving out personal or identifying details or photographs online without permission
  - recognising that people online may not be who they say they are
  - never arranging to meet someone they only know online
  - staying in public/chaperoned online spaces (e.g., supervised chat)
  - not opening attachments or downloads from unknown sources
  - knowing what to do if they see or receive something upsetting or suspicious (e.g., log off, screenshot if safe, tell a trusted adult)
- Instances of misuse or breach of acceptable use will lead to appropriate sanctions and support/education interventions.
- We review and refresh the pupil AUA annually and ensure new pupils receive it on entry.

8. Staff – Acceptable Use, Data Protection & Professional Conduct

- All staff and volunteers must follow the school's Acceptable Use Policy (AUP) for ICT, align with Staff Conduct, Online Safety, Child Protection and GDPR policies.
- Staff must:
  - Use school-provided systems/devices for educational/professional purposes; adhere to any limits on personal use as set by the school.
  - Protect their login credentials/passwords; not share them or use others' credentials.
  - Store, transfer and access personal/sensitive data in line with GDPR/data-protection policy (e.g., encrypted or password-protected when off-site).
  - Ensure photographs, videos and digital records comply with consent procedures, privacy expectations and do not identify pupils by full name or compromising detail (unless specific permission given).
  - Use personal devices for school business only when authorised, secured and in line with policy; switch off/personal phones are not used in lessons or where children are present (see Mobile Phone policy).
  - Be professional in all communications (including email, social media, remote working); only use official channels to communicate with pupils/parents unless explicit permission granted.

    - Report any concerns, breaches, damage or faults to the DSL, IT lead or appropriate person promptly.
- Breaches of acceptable use may lead to disciplinary action, in line with Staff Conduct and Safeguarding policies.

9. Incident Management, Sanctions & Support

- All online-safety incidents (in or out of school when related to school systems) will be reported, logged (e.g., via CPOMS) and reviewed by the DSL/SLT.
- We will provide support to pupils and staff affected by online-safety incidents (e.g., cyber-bullying, exploitation, radicalisation, image sharing) and engage with parents/carers when appropriate.
- Sanctions for pupils may include: withdrawal of device/network access, extra supervision, education/mentoring, referral to external agencies.
- For staff/volunteers: internal disciplinary procedures, removal of access rights, possible referral to external agencies (including police) when required.
- We will conduct post-incident review to identify lessons learned, update policy or practice as needed, and ensure filtering/monitoring systems remain effective.

10. Inclusion & Equality

- All pupils, regardless of race, gender, disability, cultural background, socio-economic status, SEND or EAL, have entitlement to access technology and online learning opportunities.
- Staff will ensure that no group is disadvantaged in use of digital technologies and will monitor patterns of access and engagement to promote equity.
- Online-safety education will be accessible and appropriate for all pupils, including those with additional needs or vulnerabilities.

11. Social Media, External Platforms & Remote Access

- We recognise that pupils under the age of 13 should not access social networking sites which require a higher minimum age (unless supervised/approved by school and parent/carer) and endeavour to remind parents and children of this fact.
- We will educate about the risks of social networking, chat rooms, message apps, live-streaming and others, including the risks from contact, content, conduct and commerce.

- Staff must follow the Acceptable Use policy and Staff Conduct policy when using social media or external platforms; they must not engage in professional communications with pupils/parents from personal accounts unless explicitly authorised.
- Remote learning platforms must be approved by the school; pupils and staff using them must comply with this policy in respect of behaviour, data protection and supervision.
- All remote access to school systems (via personal or school devices) must use secure methods, comply with the school's cyber-security policy and avoid placing the school or individuals at risk.

12. Roles & Responsibilities

Senior Leadership Team (SLT) & Governors

- Develop, own and promote the online-safety vision; make appropriate resources available.
- Receive and review online-safety incident logs; support escalation of concerns.
- Ensure the school's filtering/monitoring meets DfE standards, is regularly reviewed, and meets the school's risk profile.
- Stay up-to-date with new online-safety threats and technologies; ensure relevant training for staff and governors.
- Ensure online-safety is embedded across curriculum, culture, policies and practice, and is properly resourced.

Designated Safeguarding Lead (DSL) (Online-Safety Lead)

- Lead and coordinate online-safety within the school, in line with the Child Protection / Safeguarding policy.
- Work with IT lead, SLT, governors to manage filtering/monitoring, incident response, risk assessment and review.
- Maintain incident logs, oversee actions, liaise with external agencies where needed (e.g., police, Internet Watch Foundation, CEOP).
- Provide training, ensure staff and volunteers know their roles, promote pupil and parental engagement in online safety.

Teaching & Support Staff

- Embed online-safety education into curriculum and daily practice; model safe and positive use of technology.
- Must be aware of risks and responsibilities regarding technology, data protection, online behaviour, remote access and safeguarding.
- Identify and escalate online-safety concerns appropriately.

- Use strong passwords, lock devices when unattended; safeguard school systems, data and pupils.
- Understand and follow the school's acceptable-use agreements for staff and for pupils.

Pupils

- Understand their responsibilities with regard to safe, respectful and positive use of technology and online environments.
- Report concerns or incidents to a trusted adult.
- Use school systems and devices in line with the pupil Acceptable Use Agreement.

Parents/Carers

- Support the school's online-safety culture by reinforcing safe and responsible technology use at home.
- Engage with guidance and training provided; discuss online behaviour and risks with their children.
- Understand the school's filtering/monitoring arrangements and know how to raise concerns.

13. Monitoring, Review & Evaluation

- This policy will be reviewed annually (or sooner if significant changes in technology, legislation or school practice occur).
- We will monitor the effectiveness of online-safety education (pupil knowledge, behaviours), filtering/monitoring systems, incident logs, staff training records, and remote-learning usage.
- Filtering/monitoring provision will be reviewed at least once per academic year, considering the risk profile of pupils (including SEND, EAL, etc.), new technologies (e.g., AI), and any major change in systems or devices.
- Outcomes of monitoring and review will be reported to SLT and governors and, where relevant, will feed into the school's Self-Evaluation, Safeguarding Action Plan and improvement planning.

14. Appendices

- Appendix A: Pupil Acceptable Use Agreement
- Appendix B: Staff/Volunteer Acceptable Use Policy Agreement
- Appendix C: Incident Response Flowchart & Online-Safety Reporting Form

Glossary (selected)

- ICT: Information and Communication Technology
- DSL: Designated Safeguarding Lead
- DDSL: Deputy Designated Safeguarding Lead
- SEND: Special Educational Needs and/or Disabilities
- EAL: English as an Additional Language
- BYOD: Bring Your Own Device
- AUP: Acceptable Use Policy/Agreement
- RSHE: Relationships, Sex and Health Education
- 4 Cs (in online-safety): Content, Contact, Conduct, Commerce – as outlined in KCSIE and DfE guidance. GOV.UK Assets

Appendix A

Pupil Acceptable Use Agreement

Appendix B

Staff, Governor and Visitor Acceptable Use Agreement

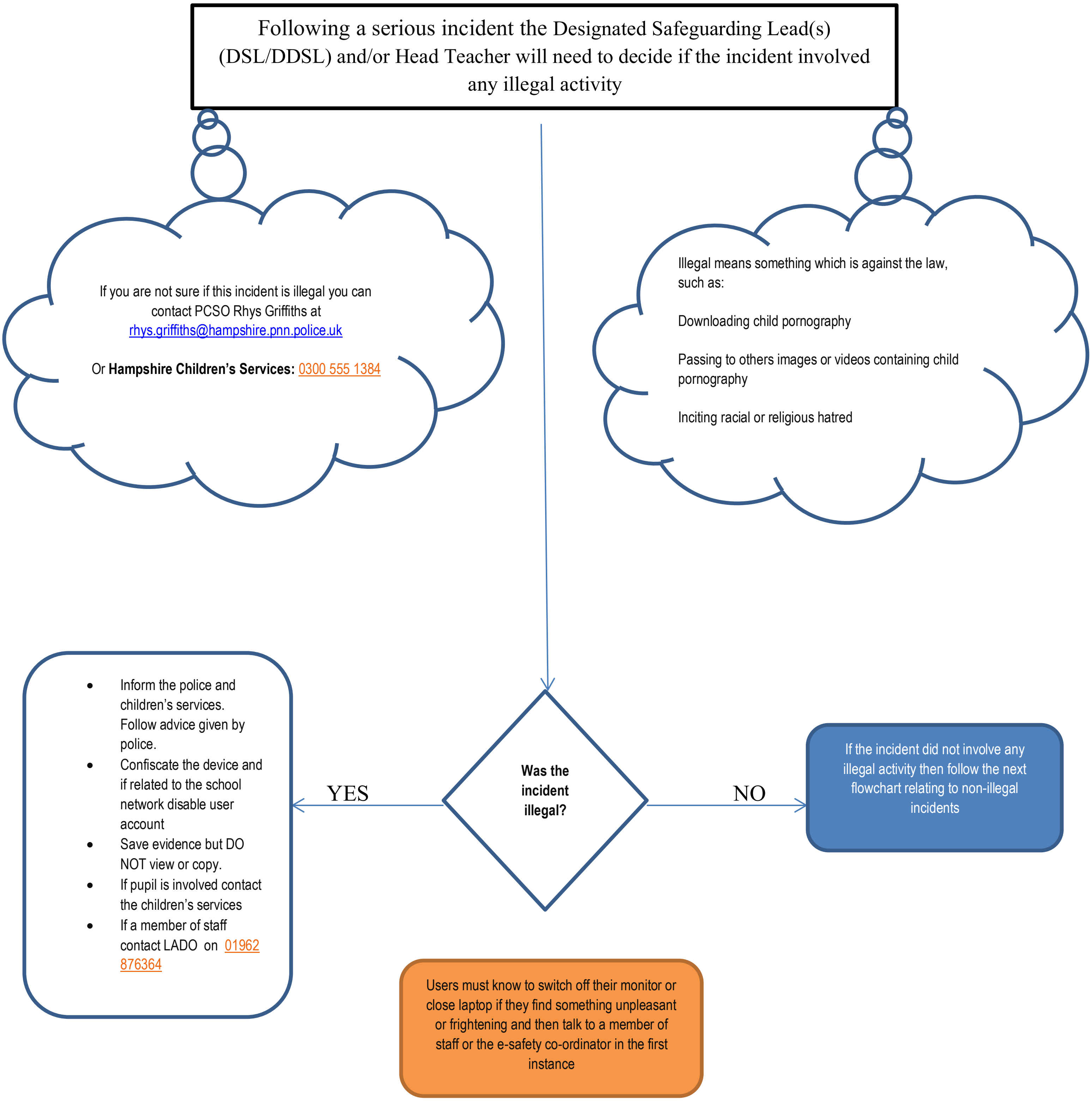
Appendix C

Response to an incident of concern

The flowchart on the next page is illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and should always be discussed with a DSL or Head Teacher

Appendix E

Flowchart for managing an illegal e-safety incident



Following a serious incident the Designated Safeguarding Lead(s) (DSL/DDSL) and/or Head Teacher will need to decide if the incident involved any illegal activity

If you are not sure if this incident is illegal you can contact PCSO Rhys Griffiths at rhys.griffiths@hampshire.pnn.police.uk

Or **Hampshire Children's Services:** 0300 555 1384

Illegal means something which is against the law, such as:

Downloading child pornography

Passing to others images or videos containing child pornography

Inciting racial or religious hatred

Was the incident illegal?

YES

- Inform the police and children's services. Follow advice given by police.
- Confiscate the device and if related to the school network disable user account
- Save evidence but DO NOT view or copy.
- If pupil is involved contact the children's services
- If a member of staff contact LADO on 01962 876364

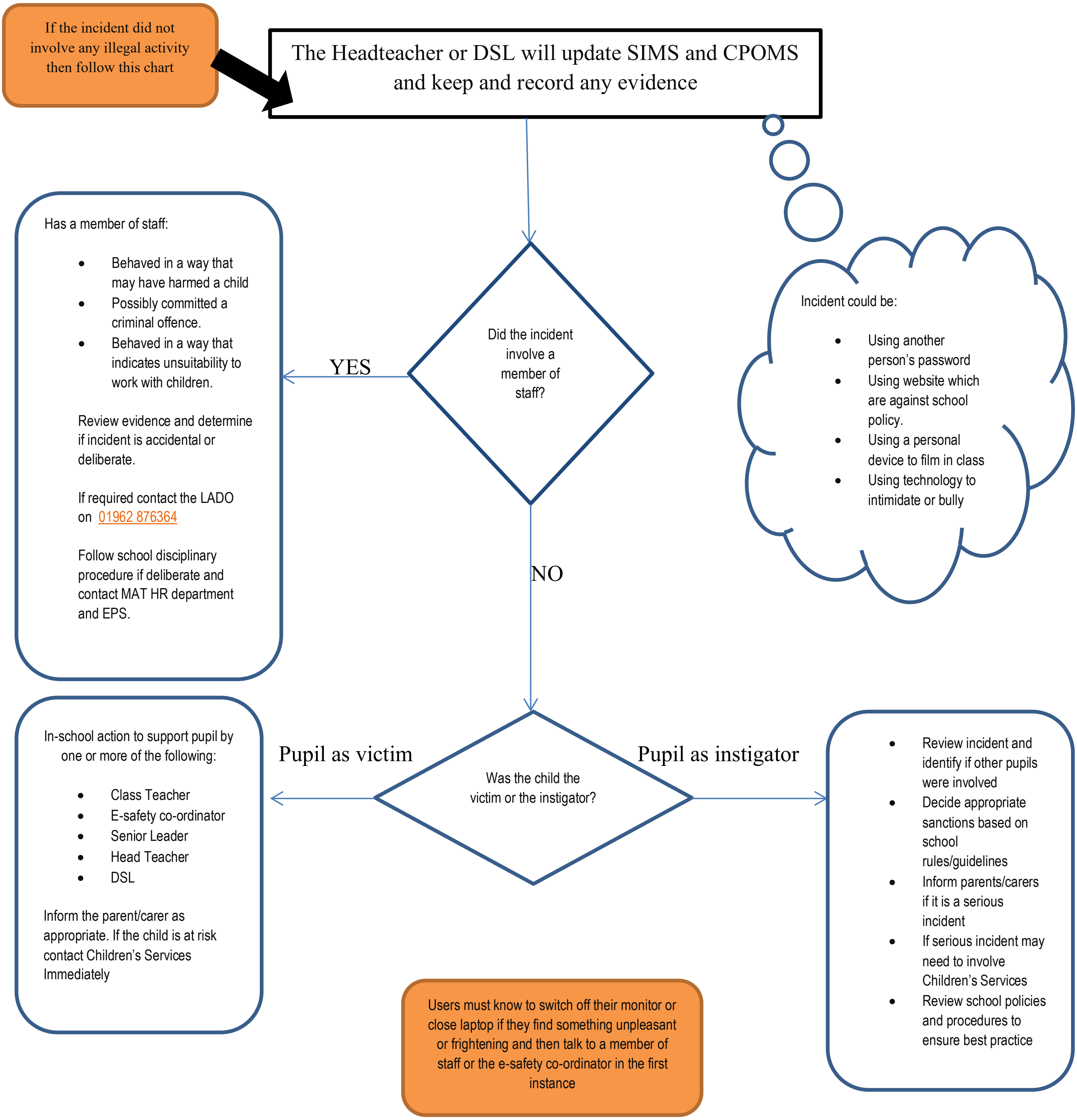
NO

If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the e-safety co-ordinator in the first instance

Appendix F

Flowchart for managing an e-safety incident to be managed in school



If the incident did not involve any illegal activity then follow this chart

The Headteacher or DSL will update SIMS and CPOMS and keep and record any evidence

Incident could be:

- Using another person's password
- Using website which are against school policy.
- Using a personal device to film in class
- Using technology to intimidate or bully

Did the incident involve a member of staff?

YES

Has a member of staff:

- Behaved in a way that may have harmed a child
- Possibly committed a criminal offence.
- Behaved in a way that indicates unsuitability to work with children.

Review evidence and determine if incident is accidental or deliberate.

If required contact the LADO on 01962 876364

Follow school disciplinary procedure if deliberate and contact MAT HR department and EPS.

NO

Was the child the victim or the instigator?

Pupil as victim

In-school action to support pupil by one or more of the following:

- Class Teacher
- E-safety co-ordinator
- Senior Leader
- Head Teacher
- DSL

Inform the parent/carer as appropriate. If the child is at risk contact Children's Services Immediately

Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions based on school rules/guidelines
- Inform parents/carers if it is a serious incident
- If serious incident may need to involve Children's Services
- Review school policies and procedures to ensure best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the e-safety co-ordinator in the first instance